ترجمة دورة كالي لينكس المجانية المقدمة من الموقع الرسمي

ترجمة:

علي العمامي

fb.com/al3mamyali

الدورة المجانية لاستكشاف نظام Kali

نصيحة: عندما يقوم مستخدم مسجل بتمييز موضوع الدورة التدريبية على أنه مكتمل، سيتم نقله إلى الموضوع التالي تلقائيًا. إذا قمت بوضع علامة على الدرس بالكامل، فسيأخذك إلى الدرس التالي، حتى لو لم تكن قد انتهيت من جميع الموضوعات. يمكنك بعد ذلك الانتقال إلى العناصر السابقة والتالية التي قرأتها بالفعل.

سيظهر لك أيضًا وضع علامة على درس أو صفحة موضوع مكتملة على تقدمك (يحتاج المستخدمون إلى تسجيل الدخول من أجل مؤشر التقدم هذا)، ويسمح لك بتتبع المكان الذي توقفت عنده.

يمكن استخدام المنتديات لطرح الأسئلة للمساعدة في أي أقسام تواجه صعوبة في فهمها، أو أي تمرين لم ينجح معك كما هو متوقع.

يرجى قراءة والبحث في الكتاب أولاً قبل تجربة أوامر من تمرين أو موضوع، وقبل نشر الأسئلة. إذا كنت لا تزال تواجه مشكلات، فقم بنشر سؤالك بالتفصيل في المنتديات، جنبًا إلى جنب مع بناء جملة الأمر الذي تستخدمه وأي مخرجات خطأ تراه على وحدة التحكم الخاصة بك.

---((نبذة مختصرة))---

يتكون Kali Linux من العديد من الأدوات القوية، ولكن لا يمكنك استخدامها بشكل جيد إذا لم تتقن نظام التشغيل الأساسي. يغطي هذا الكتاب كل ما تحتاج معرفته حتى تتمكن من استخدام Kali Linux ونشره بفعالية.

سيناقش هذا الكتاب الاستخدام الأساسي لنظام Linux للمبتدئين وإدارة حزم Debian واستخدامها وتثبيت Kali والتكوين والأمان والاستخدام المتقدم لنظام Kali بما في ذلك مدى ملاءمة Kali للمؤسسة، ودور Kali في مختلف مراحل تقييم الأمان.

سيكون بمثابة مقدمة للمبتدئين على نظام Kali ولكن أيضًا لتلبية احتياجات المستخدمين الذين يتابعون شهادات Kali والمستخدمين المتقدمين الذين يبحثون عن المزيد من حالات الاستخدام المتعمقة والإلهام.

مقدمة

في عام 1998، كنت أحد المخترقين الناجحين، وشاركت في تأسيس أحد فرق الاختراق البيضاء الأولى المحترفة. كنا أطفالًا، بالفعل، نمتلك وظائف يحلم بها، يدفع لنا لاقتحام بعض أنظمة الحاسوب والشبكات والمباني الأكثر أمانًا على هذا الكوكب.

يبدو الأمر مثيرًا للغاية، ولكن في الواقع، لقد أمضينا معظم وقتنا على لوحة مفاتيح مسلحة بالأدوات الرقمية في عملنا. لقد استخدمنا مجموعة كبيرة من البرامج، التي صممت لتعيين الشبكات وتحديد الأهداف؛ ثم مسحها واستغلالها. في بعض الحالات، يقوم أحدنا (غالبًا Jim Chapple) بكتابة أدوات مخصصة للقيام بأشياء شريرة مثل فحص شبكة من الفئة A (شيء لا تستطيع أي أداة أخرى القيام به في ذلك الوقت)، ولكن في أغلب الأحيان سوف نستخدم أو نعدل الأدوات التي كتبها مجتمع المخترقين. في تلك الأيام التي سبقت Google، ترددنا على BugTraq وAstaLaVista وStorm Packet وw00٠٠w وSecurityFocus وX-Force وغيرها من الموارد لإجراء البحوث وبناء ترسانتنا.

منذ أن كان لدينا وقت محدود في كل حفلة، كان علينا التحرك بسرعة. هذا يعني أننا لا نستطيع قضاء الكثير من الوقت في تجربة الأدوات. كان هذا يعني أننا يجب أن نتعلم الأدوات الأساسية من الداخل والخارج، وحفظ الأدوات المساعدة بحيث نصل إليها بنقرة. لقد كان هذا يعني أنه كان علينا أن نوفر أدواتنا منظمة بشكل جيد، وموثقة، ومختبرة، لذلك ستكون هناك بعض المفاجآت في هذا المجال. بعد كل شيء، إذا لم ندخل، فقدنا وجهنا مع عملائنا وسيأخذون توصياتنا بجدية أقل.

وبسبب هذا، قضيت الكثير من الوقت في فهرسة الأدوات. عندما تم إصدار أداة أو تحديثها، كنت أذهب إلى روتين. كان عليّ معرفة ما إذا كان سيتم تشغيله على منصة الهجوم (بعضها لم يكن كذلك)، وما إذا كان الأمر يستحق ذلك (لم يكن البعض)؛ اضطررت إلى تحديث أي نصوص تعتمد عليها وتوثيقها واختبارها، بما في ذلك ترحيل أي تغييرات تم إجراؤها على الإصدار السابق.

بعد ذلك، أود التخلص من جميع الأدوات ووضعها في المجلدات بناءً على الغرض منها أثناء التقييم. أود كتابة برامج نصية مجمعة لأدوات معينة، وسلاسل بعض الأدوات معًا، وربط كل ذلك في قرص مضغوط منفصل يمكن أن نأخذه في مناطق حساسة، عندما لا يسمح لنا العملاء بأخذ آلات الهجوم أو إزالة الوسائط من مختبراتهم.

كانت هذه العملية مؤلمة، لكنها كانت ضرورية. كنا نعلم أن لدينا القدرة على اقتحام أي شبكة — إذا طبقنا مهاراتنا وخبراتنا بشكل صحيح، ظللنا منظمين، وعملنا بكفاءة. على الرغم من أن البقاء غير مهزوم كان حافزًا، فقد كان يتعلق بتوفير خدمة للعملاء الذين يحتاجون إلينا لاقتحام الشبكات، حتى يتمكنوا من سد الثغرات وتحويل الأموال إلى برامج أمنية.

قضينا سنوات في شحذ مهاراتنا وخبراتنا لكننا لن ننجح دون تنظيم وكفاءة. كنا سنفشل إذا لم نتمكن من وضع أيدينا على الأداة المناسبة عند الحاجة لها.

لهذا السبب قضيت الكثير من الوقت في البحث والتوثيق والاختبار وفهرسة الأدوات، وفي نهاية القرن الحادي والعشرين، سرعان ما أصبحت وظيفة ساحقة بدوام كامل. بفضل الإنترنت، انفجر سطح الهجوم في جميع أنحاء العالم وزاد تنوع وعدد أدوات الهجوم بشكل كبير، كما زاد عبء العمل المطلوب لصيانتها.

ابتداء من عام 2004، لم ينفجر الإنترنت فقط كأساس للأعمال التجارية ولكن أيضًا كمنصة اجتماعية. كانت أجهزة الحاسوب بأسعار معقولة، وأكثر ملاءمة للمستهلكين في كل مكان. توسعت تقنية التخزين من ميغابايت إلى غيغابايت. قفزت الإيثرنت من مئات الكيلوبايت إلى عشرات ميقابايتات في الثانية، وكانت اتصالات الإنترنت أسرع وأرخص من أي وقت مضى. التجارة الإلكترونية آخذة في الازدياد، ومواقع التواصل الاجتماعي مثل (2004) Facebook و (2006) Twitter أصبحت على الإنترنت ونضجت (1998) Google إلى درجة أن أي شخص (بما في ذلك المجرمين) يمكن أن يجد أي شيء على الإنترنت.

نتيجة لذلك، أصبح البحث حاسماً بالنسبة لفرق مثل فرقنا لأنه كان علينا مواكبة الهجمات وأدوات العمل الجديدة. لقد استجبنا لمزيد من جرائم الحاسوب، وطلب عمل التحقيقات الجنائية بأن نخطو قليلاً لأننا استخفنا بالأدلة المحتملة. يعني مفهوم القرص المضغوط المباشر أننا يمكن أن نؤدي التحقيق الجنائي المباشر على جهاز بدون خطر ودون المساس بالأدلة.

الآن أصبح على فريقنا الصغير إدارة أدوات الهجوم وأدوات التحقيق الجنائي؛ كان علينا مواكبة جميع منهجيات الهجوم واستغلالها؛ وكان علينا، كما تعلمون، فعل ما فعلناه مقابل اختبارات الاختراق، التي كانت مطلوبة بشدة. كانت الأمور تخرج عن نطاق السيطرة، وقبل وقت طويل، كنا نقضي وقتاً أقل في المعركة والمزيد من الوقت في البحث، وشحذ أدواتنا، والتخطيط.

لم نكن وحدنا في هذا الصراع. في عام 2004، أصدر Mati "Muts" Aharoni، أحد المخترقين والمتخصصين في مجال الأمن ("WHoppiX" (White hat Knoppix، وهو قرص مضغوط مباشر على نظام Linux والذي وصفه بأنه "القرص المضغوط المباشر لاختبار الاختراق"، وقد تضمن "جميع الاستغلالات من SecurityFocus، Packet Storm وk-otik، إطار عمل Metasploit 2.2 والكثير الكثير. "

أتذكر تنزيل WHoppiX وأنه كان رائعا. لقد قمت بتنزيل أقراص مضغوطة مباشرة أخرى، معتقدًا أنه إذا كنت في حالة قرصنة حقيقية، فستتمكن الأقراص المضغوطة المباشرة من حفظ الـ bacon في الحقل. لكنني لم أكن على وشك الاعتماد على WHoppiX أو أي قرص مضغوط آخر للعمل الحقيقي. لم أثق في أي منهم لتلبية معظم احتياجاتي؛ لم أشعر بأن أي منهم مناسب لسير عملي؛ لم تكن توزيعات كاملة وقابلة للتثبيت؛ وفي اللحظة التي قمت بتنزيلها، كانت قديمة.

لقد أضفت ببساطة هذه الصور المضغوطة، على الرغم من حجمها الهائل نسبيًا، إلى ترسانتنا واستمريت في العملية المؤلمة المتمثلة في الحفاظ على مجموعة الأدوات "الحقيقية" الخاصة بنا.

ولكن على الرغم من آرائي الشخصية في ذلك الوقت، وربما على الرغم من توقعات Muts، كان لـ WHoppiX وتفرعاته تأثير زلزالي على حياته وعلى عملنا ومجتمعنا.

في عام 2005، تطورت WHoppiX إلى WHAX، من خلال مجموعة أدوات موسعة ومحدثة، تستند إلى "القرص المباشر الأكثر حداثة (Slackware) SLAX ". بدا أن Muts وفريق كبير من المتطوعين من مجتمع الاختراق يدركون أنه بصرف النظر عن مدى ثقتهم، لا يمكنهم أبدًا توقع كل نمو وتقلبات عملنا وأن مستخدمي القرص المضغوط لديهم احتياجات متنوعة في هذا المجال. كان من الواضح أن Muts وفريقه كانوا يستخدمون بالفعل WHAX في هذا المجال، ويبدو أنهم ملتزمون بإنجاحه. كان هذا مشجعا بالنسبة لي.

في عام 2006، دمج Muts و Max Moser وفرقهم Auditor Security Linux و WHAX في توزيعة واحدة تسمى BackTrack. لا يزال BackTrack يعتمد على SLAX، حيث استمر في النمو، مضيفًا المزيد من الأدوات والمزيد من الإطارات ودعم اللغة الموسعة والدعم اللاسلكي

المكثف وبنية قائمة تلبي احتياجات المستخدمين المبتدئين والمحترفين ونواة معدلة بشكل كبير. أصبح BackTrack هو التوزيع الأمني الرائد، لكن كثيرين ما زالوا يستخدمونه كنسخة احتياطية لـ "أدواتهم الحقيقية".

بحلول أوائل عام 2009، كان Muts وفريقه قد قاموا بتوسيع BackTrack بشكل ملحوظ إلى BackTrack 4. والآن، أصبح العمل متفرغًا في Muts، ولم يعد BackTrack قرصًا مضغوطًا مباشرًا، بل كان توزيعًا كاملاً يستند إلى Ubuntu مستفيدًا من مستودعات برامج Ubuntu. شهد التحول تطوراً مشهودا: لدى آلية تحديث BackTrack 4. بكلمات Muts الخاصة: "عند المزامنة مع حزم BackTrack الخاصة بنا، سنحصل بانتظام على تحديثات لأدوات الأمان بعد إصدارها بوقت قصير".

كانت هذه نقطة تحول. قام فريق BackTrack بالتحكم في المشاكل التي تواجه مختبري الاختراق ومحللي التحقيق الجنائي وغيرهم ممن يعملون في مجالنا. من شأن جهودهم أن تنقذنا ساعات لا تحصى وتوفر أساسًا ثابتًا، مما يسمح لنا بالعودة مرة أخرى إلى المعركة وقضاء المزيد من الوقت في القيام بالأشياء المهمة (والممتعة). نتيجة لذلك، استجاب المجتمع بالتدفق على المنتديات ويكي. كان BackTrack حقًا مجهودًا اجتماعيًا، حيث لا يزال Muts يتصدر هذا المشروع.

أصبح BackTrack 4 أخيرًا منصة للقوة الصناعية، وقد تنفست أنا وآخرين مثلي الصعداء. كنا نعرف من كثب "الألم والمعاناة" الذي كان يتحمله Muts وفريقه، لأننا كنا نراقب ذلك. نتيجة لهذا، بدأ الكثير منا باستخدام BackTrack كأساس أساسي في مجالنا. نعم، ما زلنا ملتزمين بالأدوات، وكتبنا الكود الخاص بنا، وطورنا استغلالاتنا وتقنياتنا، وبحثنا وجربنا لكننا لم نجمع فقط، حدثنا، وتحققنا من صحة وتنظيم الأدوات.

كانت BackTrack 4 R1 و R2 تنقيحات أخرى في عام 2010، مما أدى إلى إعادة إنشاء Backtrack 5 في عام 2011. لا يزال BackTrack قائمًا على Ubuntu، ويحظى باهتمام كبير مع كل إصدار، أصبح BackTrack الآن مشروعًا ضخمًا يتطلب جهدًا تطوعيًا وجهدًا من المجتمع.

ولكن أيضا التمويل. أطلق Muts برنامج Offensive Security (في عام 2006) ليس فقط لتوفير خدمات التدريب واختبار الاختراق ذات المستوى العالمي ولكن أيضًا لتوفير وسيلة للحفاظ على تطور BackTrack، وضمان بقاء BackTrack مفتوح المصدر ومجاني الاستخدام.

واصلت BackTrack نموها وتحسنها خلال عام 2012 (مع R1 و R2 و R3)، مع الحفاظ على نواة Ubuntu وإضافة مئات من الأدوات الجديدة، بما في ذلك أدوات الاستغلال المادي والأجهزة، ودعم VMware، وعدد لا يحصى من برامج تشغيل الأجهزة اللاسلكية والعديد من تحسينات الاستقرار و اصلاحات الأخطاء. ومع ذلك، بعد إصدار R3، أصبح تطوير BackTrack هادئًا نسبيًا، وبشكل غامض إلى حد ما.

كان هناك بعض التكهنات في هذه الصناعة. اعتقد البعض أن شركة BackTrack بيعت، كانت شركة Offensive Security تتحول إلى واحدة من أكثر شركات التدريب احتراماً وشهرة في مجالنا، وتوقع البعض أن نجاحها قد استحوذ على مطوري BackTrack الرئيسيين وتجاهلهم. ومع ذلك، لا شيء يمكن أن يكون أبعد عن الحقيقة.

في عام 2013، تم إصدار Kali Linux 1.0. من ملاحظات الإصدار: "بعد عام من التطوير الصامت، تفخر Offensive Security بالإعلان عن إطلاق Kali Linux وتوافره على نطاق واسع، وهو التوزيع الأكثر تطوراً وقوةً واستقرارًا لاختبار الاختراق. Kali هي أكثر نضجا وآمنة ومؤسسة من BackTrack. "

Kali لم يكن مجرد إعادة صياغة للعلامة التجارية BackTrack. لقد كان فيها أكثر من 600 أداة، من الواضح أنها مجموعة أدوات رائعة، ولكن لا يزال هناك الكثير منها. تم بناء Kali، من

الألف إلى الياء، على قلب Debian. قد لا يبدو هذا شيئ كبير. لكن آثاره كان مذهل. بفضل جهد إعادة التعبئة الهائل، يمكن لمستخدمي Kali تنزيل المصدر لكل أداة على حدة؛ يمكنهم تعديل وإعادة بناء أداة حسب الحاجة، مع بضع ضغطات المفاتيح فقط. على عكس أنظمة التشغيل الرئيسية الأخرى اليوم، تزامن Kali Linux مع مستودعات Debian أربع مرات في اليوم، مما يعني أنه يمكن لمستخدمي Kali الحصول على تحديثات الحزمة الحالية وإصلاحات الأمان. قام مطورو Kali بالتجربة والتعبئة والمحافظة على الإصدارات الأولية للعديد من الأدوات بحيث ظل المستخدمون دائمًا يحصلون على التحديثات الجديدة. بفضل جذور Debian، يمكن لمستخدمي Kali بدء تثبيت أو تشغيل صورة ISO مباشرة من المستودعات، مما فتح الباب أمام عمليات تثبيت Kali المخصصة بالكامل أو عمليات النشر الضخمة للمؤسسة، والتي يمكن أن تتم أتمتتها وتخصيصها بشكل أكبر مع ملفات ما قبل البذور. لإكمال التخصيص، يمكن لمستخدمي Kali تعديل بيئة سطح المكتب وتعديل القوائم وتغيير الأيقونات وحتى تغيير بيئات النوافذ. فتحت دفعة هائلة لتطوير ARM الباب لتثبيت Kali Linux على مجموعة واسعة من منصات الأجهزة بما في ذلك نقاط الوصول وأجهزة الحواسيب أحادية اللوحة (Raspberry Pi و ODROID و BeagleBone و CubieBoard، على سبيل المثال) **وأجهزة Chromebook المستندة إلى ARM.** وأخيراً وليس آخراً، قامت Kali Linux بتحديثات بسيطة وكبيرة غير ملحوظة مما يعني أنه لن يضطروا أبدًا إلى إعادة تثبيت إعدادات Kali Linux المخصصة.

في الأيام الخمسة الأولى، قام 90.000 منا بتنزيل Kali 1.0.

هذه كانت البداية فقط. في عام 2015، تم إصدار Kali 2.0، تليها الإصدار المستمر عام 2016. باختصار، "إذا كان Kali 1.0 يركز على بناء بنية تحتية قوية، فإن Kali 2.0 يركز على إصلاح تجربة المستخدم والحفاظ على مستجدات الحزم ومستودعات الأدوات".

الإصدار الحالي من Kali Linux هو توزيع مستمر (Rolling)، والذي يمثل نهاية الإصدارات الثابتة. الآن، يتم تحديث المستخدمين باستمرار ويتلقون تحديثات وتصحيحات فور إنشائها. يتم تحديث الأدوات الأساسية بشكل دوري، وتم توفير تحسينات في إمكانية الوصول للمعاقين بصريًا، ويتم تحديث وتصحيح نواة Linux لمواصلة دعم الحقن اللاسلكية 802,11. تضيف أدوات (SDR) واتصال المجال القريب (NFC) دعمًا للحقول الجديدة لاختبار الأمان. تتوفر خيارات التثبيت الكامل للقرص المشفر لنظام Linux **وخيارات التدمير الذاتي لحالات الطوارئ،** وذلك بفضل LVM وLUKS على التوالي، وتمت إضافة خيارات ثبات USB، مما يسمح بتثبيت Kali المستندة إلى USB للحفاظ على التغييرات بين إعادة التشغيل، سواء كان محرك أقراص USB مشفرًا أم لا. أخيرًا، فتحت الإصدارات الحديثة من Kali الباب لـ NetHunter، وهو نظام تشغيل مفتوح المصدر من الطراز العالمي يعمل على الأجهزة المحمولة القائمة على Kali Linux وAndroid.

لقد تطورت Kali Linux ليس فقط إلى نظام الاختبار المحترف في أمن المعلومات، بل إلى نظام تشغيل عالمي وناضج وآمن وجاهز للمؤسسات.

من خلال عملية التطوير التي استمرت لعقد من الزمن، تحمل Muts وفريقه، إلى جانب التفاني الدؤوب من عدد لا يحصى من المتطوعين من مجتمع المخترقين، عبء تبسيط وتنظيم بيئة عملنا، وتحريرنا من الكثير من كدح عملنا وتوفير أساس آمن وموثوق، مما يسمح لنا بالتركيز على دفعنا إلى الأمام نحو الهدف النهائي المتمثل في تأمين عالمنا الرقمي.

ومن المثير للاهتمام، ولكن ليس من المستغرب، أن مجتمعًا مدهشًا قد بنى Kali Linux. كل شهر، ثلاثة إلى أربعمائة ألف منا ينزلون نسخة من Kali. نجتمع معًا في منتديات Kali، التي يبلغ عددهم أربعين ألف شخص، ويمكن العثور على ثلاث إلى أربعمائة منا في وقت واحد على قناة

Kali. نجتمع في المؤتمرات وحضور Kali Dojos لمعرفة كيفية الاستفادة من Kali بشكل أفضل من المطورين أنفسهم.

غير Kali Linux عالم أمن المعلومات للأفضل، وقد أنقذ Muts وفريقه كل واحد منا ساعات لا تحصى من الكد والإحباط، مما سمح لنا بقضاء المزيد من الوقت والطاقة في دفع إنتاجنا للأمام، معًا.

لكن على الرغم من قبولها ودعمها وشعبيتها المذهلة، لم تصدر Kali دليلًا رسميًا. حسنا، الآن بعد أن تغير. يسرني أن أكون إلى جانب فريق التطوير Kali وبالتحديد Mati Aharoni و Raphaël Hertzog و Devon Kearns و Jim O'Gorman لتقديم هذا، وهو الأول في سلسلة من المنشورات الرسمية التي ربما تركز على Kali Linux. في هذا الكتاب، سنركز على منصة Kali Linux نفسها، وسنساعدك على فهم وتعظيم استخدام Kali من الألف إلى الياء. لن نتعمق في ترسانة الأدوات الموجودة في Kali Linux، ولكن سواء كنت مخضرمًا أو مبتدئا، فهذا هو أفضل مكان للبدء، إذا كنت جاهزًا للدخول والحصول على تجربة جدية مع Kali Linux. بغض النظر عن المدة التي قضيتها في التجربة، فإن قرارك بقراءة هذا الكتاب يربطك بمجتمع Kali Linux المتنامي، أحد أقدم وأكبر وأكثر نشاطًا وحيوية في مجالنا.

نيابة عن Muts وبقية فريق Kali المذهل، تهانينا على اتخاذ الخطوة الأولى لإتقان Kali Linux!

جوني لونج

فبراير 2017

---((مقدمة لنظام Kali Linux))---

مقدمة

Kali Linux هي أقوى وأشهر منصة للاختراق في العالم، ويستخدمها متخصصو الأمن في مجموعة واسعة من التخصصات، بما في ذلك اختبار الاختراق، والتحقيق الجنائي، والهندسة العكسية، وتقييم الثغرات الأمنية. إنها تتويجا لسنوات من التحسينات ونتيجة للتطور المستمر للمنصة، من WHoppiX إلى WHAX، إلى BackTrack، والآن إلى إطار اختبار الاختراق الكامل الذي يستفيد من العديد من ميزات Debian GNU / Linux ومجتمع المصادر المفتوحة النابضة بالحياة في جميع أنحاء العالم.

لم يتم تصميم Kali Linux ليكون مجموعة بسيطة من الأدوات فقط، بل هو إطار مرن يمكن لمهنيين اختبار الاختراق المحترفين وعشاق الأمن والطلاب والهواة تخصيصه ليلائم احتياجاتهم الخاصة.

١. لماذا هذا الكتاب؟

Kali Linux ليس مجرد مجموعة من أدوات أمان المعلومات المختلفة التي يتم تثبيتها على قاعدة Debian القياسية وتم تكوينها مسبقًا للحصول على أحدث المعلومات وتشغيلها على الفور. للحصول على أقصى استفادة من Kali، من المهم أن يكون لديك فهم شامل لأسس GNU / Debian Linux القوية (التي تدعم جميع تلك الأدوات الرائعة) وتعلم كيف يمكنك استخدامها في بيئتك.

على الرغم من أن Kali متعددة الأغراض، إلا أنها مصممة بشكل أساسي للمساعدة في اختبار الاختراق. الهدف من هذا الكتاب ليس فقط مساعدتك على الشعور بأنك في بيتك عند استخدام Kali Linux، ولكن أيضًا للمساعدة في تحسين فهمك وتبسيط تجربتك، بحيث عندما تشارك في اختبار الاختراق ويكون الوقت ضروريًا، لا داعي للقلق بشأن فقدان دقائق ثمينة لتثبيت برنامج جديد أو تمكين خدمة شبكة جديدة. في هذا الكتاب، سنقدمك أولاً إلى Linux، ثم سنغطس بشكل أعمق ونحن نقدم لك الفروق الدقيقة الخاصة بـ **Kali Linux** حتى تعرف بالضبط ما يجري تحت الغطاء.

هذه معرفة لا تقدر بثمن، لا سيما عندما تحاول العمل في ظل قيود زمنية ضيقة. ليس من غير المألوف طلب هذا العمق من المعرفة عندما تقوم بالإعداد، أو استكشاف الأخطاء وإصلاحها، أو تكافح لثني أداة لإرادتك، أو تحليل الناتج من أداة، أو الاستفادة من Kali في بيئة واسعة النطاق.

2. هل هذا الكتاب يناسبك؟

إذا كنت تريد الغوص في مجال أمن المعلومات الثري بشكل لا يصدق، وقمت باختيار Kali Linux بحق كمنصة أساسية، فإن هذا الكتاب سيساعدك في هذه الرحلة. تم كتابة هذا الكتاب لمساعدة مستخدمي Linux لأول مرة، وكذلك مستخدمي Kali الحاليين الذين يسعون إلى تعميق معرفتهم بأساسات Kali، وكذلك أولئك الذين استخدموا Kali لسنوات لكنهم يتطلعون إلى إضفاء الطابع الرسمي على تعلمهم، وتوسيع نطاقهم استخدام Kali، وملء الثغرات في معرفتهم.

بالإضافة إلى ذلك، يمكن أن يكون هذا الكتاب بمثابة خارطة طريق ومرجع فني ودليل دراسة لمن يتبعون شهادة "Kali Linux Certified Professional "KLCP.

3. النهج العام وهيكل الكتاب

تم تصميم هذا الكتاب بحيث يمكنك وضع يديك على Kali Linux من البداية. ليس عليك قراءة نصف الكتاب للبدء. تتم تغطية كل موضوع بطريقة عملية للغاية، والكتاب مليء بالعينات ولقطات الشاشة للمساعدة في جعل التفسيرات مفهومة أكثر.

الفصل ١: حول Kali Linux، يعرف بعض المصطلحات الأساسية ويشرح الغرض من Kali Linux.

الفصل ٢: "بدء استخدام Kali Linux" يرشدك خطوة بخطوة من تنزيل صورة ISO إلى تشغيل Kali Linux على الحاسوب الخاص بك.

الفصل ٣: أساسيات Linux التي تحتاج لمعرفتها عن أي نظام Linux، مثل بنيته، وعملية التثبيت، والتسلسل الهرمي لنظام الملفات، والأذونات، وأكثر من ذلك. في هذه المرحلة، ستستخدم Kali Linux كنظام مباشر لفترة من الوقت.

الفصل ٤: تثبيت Kali Linux يوضح لك كيفية إجراء تثبيت Kali Linux دائم (على القرص الثابت الخاص بك).

الفصل ٥: تكوين Kali Linux وكيفية تغييره حسب رغبتك. كمستخدم منتظم لـ Kali، فقد حان الوقت للتعرف على الموارد المهمة المتاحة لمستخدمي Kali.

الفصل ٦: الحصول على المساعدة، يمنحك المفاتيح للتعامل مع المشاكل غير المتوقعة التي من المحتمل أن تواجهها.

مع الأساسيات المغطاة جيدًا، يغطس باقي الكتاب في موضوعات أكثر تقدمًا:

الفصل ٧: تأمين ومراقبة Kali Linux يمنحك نصائح للتأكد من أن تثبيت Kali Linux يفي بمتطلبات الأمان الخاصة بك.

الفصل ٨: يشرح إدارة حزم Debian كيفية الاستفادة من الإمكانات الكاملة لنظام التغليف في Debian.

الفصل ٩: Advanced Usage، تتعلم كيفية إنشاء صورة Kali Linux ISO مخصصة بالكامل. كل هذه المواضيع تكون أكثر صلة عندما تقوم بنشر Kali Linux على نطاق واسع في مؤسسة كما هو موثق في **الفصل ١٠**، Kali Linux في المؤسسة.

الفصل الأخير - الفصل ١١، مقدمة في تقييمات الأمان - يجعل الرابط بين كل ما تعلمته في هذا الكتاب والعمل اليومي لمحترفي الأمن.

يعد العمل في هذا الكتاب أيضًا فرصة رائعة قدمها لي ماتي. إنه ليس نفس النوع من العمل، لكن من المفيد بنفس القدر أن نكون قادرين على مساعدة الناس ومشاركتهم خبرتي في نظام التشغيل Kali / Debian. بناءً على تجربتي مع كتيب إدارة Debian، آمل أن تساعدك توضيحاتي على البدء في عالم سريع الحركة لأمن الحاسوب.

---((الفصل الأول))---

1. حول Kali linux

Kali Linux هي توزيعة Linux للتدقيق الأمني جاهزة للشركات تستند على Debian GNU / Linux. يهدف Kali إلى متخصصي الأمن ومسؤولي تقنية المعلومات، مما يمكنهم من إجراء اختبارات الاختراق المتقدمة والتحقيق الجنائي وتدقيق الأمان.

ما هي توزيعات لينكس؟

على الرغم من أنه يستخدم بشكل شائع كاسم لنظام التشغيل بالكامل، إلا أن Linux هو مجرد اسم للنواة (kernel) فقط، وهو برنامج يربط بين الهاردوير وتطبيقات المستخدم النهائي.

يشير مصطلح توزيعة Linux، من ناحية أخرى، إلى نظام تشغيل كامل مبني على نواة Linux، وعادة ما يتضمن برنامج تثبيت والعديد من التطبيقات، إما مثبتة مسبقًا أو مغلفة بطريقة سهلة التثبيت.

Debian GNU / Linux هي إحدى توزيعات Linux الشائعة، معروفة بجودتها واستقرارها. يستند Kali Linux على Debian ويضيف أكثر من 300 حزمة من الأدوات الخاصة، وكلها تتعلق بأمن المعلومات، لا سيما مجال اختبار الاختراق.

Debian هو مشروع برمجي مجاني يوفر إصدارات متعددة من نظام التشغيل الخاص به، وغالبًا ما نستخدم مصطلح التوزيعة للإشارة إلى إصدار محدد منه، على سبيل المثال توزيعات Debian Stable أو Debian Testing. وينطبق الشيء نفسه أيضًا على Kali Linux أيضا — على سبيل المثال Kali Rolling.

1.1 نبذة عن تاريخ Kali

بدأ مشروع Kali Linux بهدوء في عام 2016، عندما قرر Offensive Security أن يحلوا محل مشروع BackTrack Linux الموقر، والذي تمت صيانته يدويًا، بشيء يمكن أن يصبح فرعا من Debian، مع اكمال جميع البنية التحتية المطلوبة وتقنيات التغليف المحسنة. تم اتخاذ القرار لبناء Kali مستندا على Debian؛ لأنه معروف بجودته واستقراره وتوفيره لمجموعة واسعة من البرامج المتاحة. لهذا السبب شارك (Raphaël) في هذا المشروع، كمستشار لديبيان.

حدث الإصدار الأول (الإصدار 1.0) بعد عام واحد، في مارس 2013، واستند على Debian "Wheezy 7"، التوزيعة الثابتة لـ Debian في ذلك الوقت. في تلك السنة الأولى من التطوير، قمنا بتعبئة مئات التطبيقات المتعلقة باختبار الاختراق وبنينا البنية التحتية. على الرغم من أن عدد التطبيقات كبير، إلا أنه تم تنسيق قائمة التطبيقات بدقة، حيث تم إسقاط التطبيقات التي لم تعد تعمل أو تلك الميزات المكررة المتوفرة بالفعل في برامج أفضل.

خلال العامين التاليين للإصدار 1.0، أصدرت Kali العديد من التحديثات الإضافية، مما أدى إلى توسيع نطاق التطبيقات المتاحة وتحسين دعم الأجهزة، وذلك بفضل إصدارات النواة الأحدث. مع بعض الاستثمار في التكامل المستمر، تأكدنا من أن جميع الحزم المهمة كانت محفوظة في حالة قابلة للتثبيت وأنه يمكن دائمًا إنشاء صور مباشرة مخصصة (خاصية مميزة للتوزيعة).

في عام 2015، عندما خرج Debian 8 "Jessie"، عملنا على إعادة تطبيق Kali Linux. على الرغم من أن Kali Linux 1.x تجنب GNOME Shell (بالاعتماد على GNOME Fallback بدلاً من ذلك)، فقد قررنا في هذا الإصدار احتضانه وتحسينه: لقد أضفنا بعض امتدادات GNOME Shell لاكتساب ميزات مفقودة، وعلى الأخص قائمة التطبيقات. أصبحت نتيجة هذا العمل Kali Linux 2.0، التي نُشرت في أغسطس 2015.

جنوم هي بيئة سطح المكتب الافتراضية لـ Kali linux

كان هذا سابقا أما الأن في نهاية 2019 أصبحتxfce

تعد بيئة سطح المكتب عبارة عن مجموعة من التطبيقات الرسومية التي تشترك في مجموعة أدوات رسومية شائعة والتي تهدف إلى استخدامها معًا في محطات عمل المستخدم. لا تستخدم بيئات سطح المكتب بشكل عام في الخوادم. وهي توفر عادةً تطبيق shell، مدير ملفات، متصفح ويب، عميل بريد إلكتروني، ومجموعة برامج المكتب، إلخ.

بجانب ذلك قمنا بزيادة جهودنا لضمان حصول Kali Linux دائمًا على أحدث إصدار من جميع تطبيقات اختبار الاختراق. لسوء الحظ، كان هذا الهدف يخالف خصوصيات Debian Stable كقاعدة للتوزيعة، لأنه تطلب منا إعادة دعم العديد من الحزم. هذا يرجع إلى حقيقة أن Debian Stable تضع أولويتها على ثبات البرنامج، وغالبًا ما تتسبب في تأخير طويل من إصدار التحديث الأولي إلى عندما يتم دمجها في التوزيع. نظرًا لاستمرارنا في التكامل المستمر، كان من الطبيعي جدًا إعادة تطبيق Kali Linux على Debian testing حتى نتمكن من الاستفادة من أحدث إصدار من حزم Debian بمجرد توفرها. يحتوي Debian testing على دورة تحديث أكثر قوة، وهو أكثر توافقًا مع أهداف Kali Linux.

هذا، في جوهره، مفهوم Kali Rolling. بينما كان التوزيع المتداول متاحًا لفترة طويلة، فإن Kali 2016.1 كان أول إصدار يحتضن رسميًا الطبيعة المتداولة لهذا التوزيع: عندما تقوم بتثبيت أحدث إصدار من Kali، يتعقب نظامك فعليًا توزيع Kali Rolling وكل يوم تحصل عليه تحديثات جديدة. في الماضي، كانت إصدارات Kali عبارة عن لقطات لتوزيع Debian Stable مع حزم Kali الخاصة التي تم حقنها فيه.

يحتوي التوزيع المستمر "Rolling" على العديد من الفوائد، ولكنه يأتي أيضًا مع تحديات متعددة، سواء بالنسبة للذين يقومون ببناء التوزيعة أو للمستخدمين الذين يضطرون إلى التعامل مع تدفق لا نهائي من التحديثات وأحيانًا إلى تغييرات غير متوافقة مع الإصدارات السابقة. يهدف هذا الكتاب إلى تزويدك بالمعرفة المطلوبة للتعامل مع كل ما قد تواجهه أثناء إدارة تثبيت Kali Linux.

2.1. علاقة Kali بـ Debian

تستند توزيعة Kali Linux على Debian testing. لهذا، تأتي معظم الحزم المتوفرة في Kali Linux مباشرة من مستودع Debian هذا.

بينما تعتمد Kali Linux اعتمادًا كبيرًا على Debian، فهي أيضًا مستقلة تمامًا، بمعنى أن لدينا بنية تحتية خاصة بنا ونحتفظ بحرية إجراء أي تغييرات نريدها.

1.2.1. تدفق الحزم

من جانب Debian، يعمل المطورون كل يوم على تحديث الحزم وتحميلها على توزيعة Debian unstable. من هناك، تنتقل الحزم إلى توزيع Debian testing بمجرد التخلص من أكثر الأخطاء إثارة للمشاكل. تضمن عملية الترحيل أيضًا عدم كسر التبعيات في Debian testing. الهدف هو أن الاختبار يكون دائمًا في حالة قابلة للاستخدام (أو حتى يمكن إعادة تشغيله!).

تتوافق أهداف Debian testing جيدًا مع أهداف Kali Linux، لذا اخترناها كقاعدة.

لإضافة الحزم الخاصة بـ Kali في التوزيعة، نتبع عملية من خطوتين.

أولاً، نأخذ Debian testing ونحقن حزم Kali الخاصة بنا فيه (الموجودة في مستودع kali-dev-only) لبناء مستودع kali-dev. ستتوقف هذا الحزم من وقت لآخر: على سبيل المثال، قد لا تكون حزم Kali الخاصة بنا قابلة للتثبيت حتى يتم إعادة تجميعها مقابل المكتبات الأحدث. في حالات أخرى، قد يلزم أيضًا تحديث الحزم التي قمنا بتشكيلها، إما لتصبح قابلة للتثبيت مرة أخرى، أو لإصلاح قابلية تثبيت حزمة أخرى تعتمد على إصدار أحدث من الحزمة forked. في أي حال، ليست kali-dev للمستخدمين النهائيين.

2.2.1. إدارة الفرق مع Debian

كقرار تصميم، نحاول تقليل عدد الحزم المتفرعة إلى أقصى حد ممكن. ومع ذلك، من أجل تنفيذ بعض الميزات الفريدة لـKali، يجب إجراء بعض التغييرات.

للحد من تأثير هذه التغييرات، نحن نسعى جاهدين لإرسالها في مرحلة أخرى، إما عن طريق دمج الميزة مباشرة، أو عن طريق إضافة الروابط المطلوبة بحيث يكون من السهل تمكين الميزات المطلوبة دون مزيد من تعديل الحزم الأولية نفسها.

يساعدنا Kali Package Tracker على تتبع اختلافاتنا مع Debian. في أي وقت، يمكننا البحث عن الحزمة التي تفرعت وما إذا كانت متزامنة مع Debian أو لا، أو إذا كان التحديث مطلوباً أو لا. يتم الاحتفاظ بكل حزمنا في مستودعات Git التي تستضيف فرع Debian وفرع Kali جنباً إلى جنب. وبفضل هذا، فإن تحديث حزمة متفرعة هو عملية بسيطة من خطوتين: تحديث فرع Debian ثم دمجها في فرع Kali.

في حين أن عدد الحزم المتفرعة في Kali منخفضة نسبياً، فإن عدد الحزم الإضافية مرتفع إلى حد ما: في أبريل 2017 كان هناك ما يقرب من 400 حزمة. معظم هذه الحزم عبارة عن برامج مجانية تتوافق مع إرشادات Debian للبرمجيات الحرة وسيكون هدفنا النهائي هو الحفاظ على تلك الحزم في Debian متى ما أمكن ذلك. لهذا السبب نسعى جاهدين لامتثال سياسة Debian واتباع ممارسات التعبئة الجيدة المستخدمة في Debian. لسوء الحظ، هناك أيضًا بعض الاستثناءات القليلة التي كان من المستحيل إنشاء التغليف المناسب فيها. نتيجة لضيق الوقت، تم دفع عدد قليل من الحزم إلى Debian.

3.1. الغرض منه وحالات استخدامه

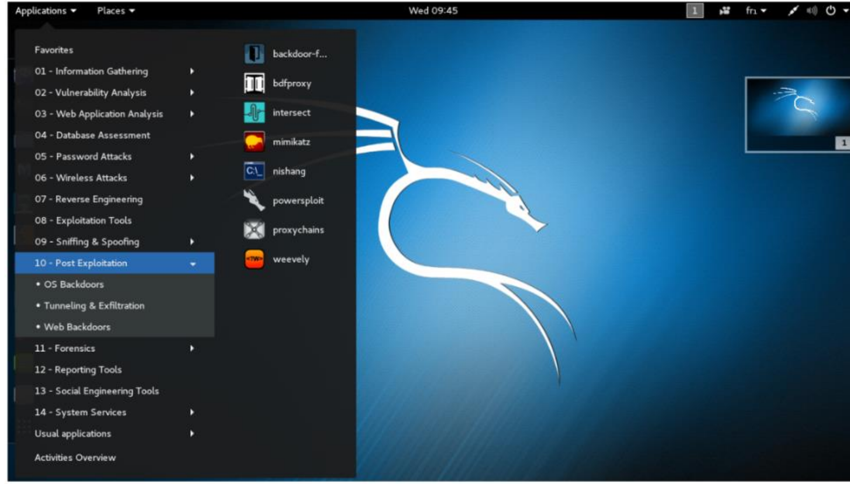
بينما يمكن تلخيص تركيز Kali باختصار على أنه "اختبار الاختراق والتدقيق الأمني"، هناك العديد من المهام المختلفة التي تنطوي عليها هذه الأنشطة. تم تصميم Kali Linux كإطار عمل، لأنه يشتمل على العديد من الأدوات التي تغطي حالات استخدام مختلفة تمامًا.

على سبيل المثال، يمكن استخدام Kali Linux على أنواع مختلفة من أجهزة الحاسوب: بالتأكيد أجهزة الحاسوب المحمولة، وأيضًا على خوادم مسؤولي النظام الذين يرغبون في مراقبة شبكاتهم، وعلى محطات عمل محللي التحقيق الجنائي، وبشكل غير متوقع، على الأجهزة المضمنة المخفية، عادةً مع وحدات المعالجة المركزية ARM، التي يمكن إسقاطها في نطاق شبكة لاسلكية أو توصيلها في جهاز الحاسوب الخاص بالمستخدمين المستهدفين. العديد من أجهزة ARM هي أيضًا آلات هجوم مثالية نظرًا لحجمها الصغير ومتطلبات الطاقة المنخفضة.

يمكن أيضًا نشر Kali Linux في السحابة لإنشاء مجموعة من آلات تكسير كلمة المرور، وعلى الهواتف المحمولة والأجهزة اللوحية للسماح باختبار الاختراق المحمول بحق.

ولكن هذا ليس كل شيء؛ يحتاج اختبار الاختراق أيضًا إلى خوادم: لاستخدام برنامج تعاون ضمن فريق من اختبار الاختراق، لإعداد خادم ويب لاستخدامه في حملات التصيد الاحتيالي، لتشغيل أدوات مسح الثغرات الأمنية وغيرها من الأنشطة ذات الصلة.

بمجرد تشغيل Kali، ستكتشف بسرعة أن قائمة Kali Linux الرئيسية مرتبة حسب الخاصيات حسب مختلف أنواع المهام والأنشطة ذات صلة بمختبري الاختراق وغيرهم من متخصصي أمن المعلومات كما هو موضح في الشكل ١.١."قائمة تطبيقات Kali Linux" التالية.



الشكل ١.١. قائمة تطبيقات Kali linux

تشمل هذه المهام والأنشطة:

❖ **جمع المعلومات (Information Gathering):** جمع البيانات حول الشبكة المستهدفة وهيكلها، وتحديد أجهزة الحاسوب، وأنظمة التشغيل الخاصة بهم، والخدمات التي يقومون بتشغيلها. تحديد الأجزاء التي يحتمل أن تكون حساسة في نظام المعلومات. استخراج جميع أنواع القوائم من مجلد تشغيل الخدمات.

❖ **تحليل الثغرات الأمنية (Vulnerability Analysis):** اختبار ما إذا كان النظام المحلي أو البعيد يتأثر بعدد من الثغرات الأمنية المعروفة أو التكوينات غير الآمنة. تستخدم ماسحات عدم الحصانة قواعد البيانات التي تحتوي على آلاف التواقيع لتحديد نقاط الضعف المحتملة.

❖ **تحليل تطبيقات الويب (Web Application Analysis):** تحديد التكوينات الخاطئة والضعف الأمني في تطبيقات الويب. من الضروري تحديد هذه المشكلات وتخفيفها نظراً لأن هذه التطبيقات توفر للجمهور مما يجعلها أهدافاً مثالية للمهاجمين.

❖ **تقييم قاعدة البيانات (Database Assessment):** من حقن SQL إلى مهاجمة بيانات الاعتماد، تعد هجمات قاعدة البيانات هدفا شائعًا للغاية للمهاجمين. يمكنك العثور على

الأدوات التي تختبر أهداف الهجوم التي تتراوح من حقن SQL إلى استخراج البيانات وتحليلها هنا.

- ❖ **هجمات كلمة المرور (Password Attacks):** أنظمة المصادقة دائمًا معرضة للهجوم. يمكن العثور هنا على العديد من الأدوات المفيدة، بدءًا من أدوات الهجوم على كلمات المرور عبر الإنترنت إلى الهجمات التي لا تعمل في وضع عدم الاتصال على أنظمة التشفير أو التجزئة.
- ❖ **الهجمات اللاسلكية (Wireless Attacks)**: تعني الطبيعة الواسعة الانتشار للشبكات اللاسلكية أنها ستكون دائمًا هدفا شائعًا للهجوم. بفضل النطاق الواسع من الدعم لبطاقات لاسلكية متعددة، تعد Kali خيارًا واضحًا للهجمات ضد أنواع متعددة من الشبكات اللاسلكية.
- ❖ **الهندسة العكسية (Reverse Engineering):** الهندسة العكسية هي نشاط له أغراض عديدة. دعما للأنشطة الهجومية، فهي واحدة من الطرق الأساسية لتحديد نقاط الضعف واستغلال تطويرها. على الجانب الدفاعي، يتم استخدامها لتحليل البرامج الضارة المستخدمة في الهجمات المستهدفة. في هذه المرحلة، الهدف هو تحديد قدرات قطعة معينة من الحرف اليدوية.
- ❖ **أدوات الاستغلال (Exploitation Tools):** تتيح لك الاستغلال، أو الاستفادة من ثغرة أمنية (تم التعرف عليها سابقًا)، التحكم في آلة بعيدة (أو جهاز). يمكن بعد ذلك استخدام هذا الوصول لمزيد من هجمات تصعيد الامتيازات، إما محليًا على الجهاز المصاب، أو على أجهزة أخرى يمكن الوصول إليها على نفس الشبكة. تحتوي هذه الفئة على عدد من الأدوات والأدوات المساعدة التي تعمل على تبسيط عملية كتابة استغلالاك الخاصة.
- ❖ **الشم والخداع (Sniffing & Spoofing)**: يعد الوصول إلى البيانات أثناء انتقالها عبر الشبكة مفيدًا للمهاجمين. يمكنك هنا العثور على أدوات الخداع التي تتيح لك انتحال شخصية

مستخدم شرعي بالإضافة إلى أدوات شم تسمح لك بالتقاط وتحليل البيانات مباشرةً من السلك. عند استخدامها معًا، يمكن أن تكون هذه الأدوات قوية جدًا.

❖ **مرحلة ما بعد الاستغلال (Post Exploitation):** بمجرد حصولك على حق الوصول إلى نظام ما، فإنك تريد غالبًا الحفاظ على هذا المستوى من الوصول أو توسيع نطاق التحكم من خلال التنقل بشكل جانبي عبر الشبكة. الأدوات التي تساعد في تحقيق هذه الأهداف موجودة هنا.

❖ **التحقيق الجنائي (Forensics):** كانت بيئات الإقلاع المباشر (التحقيق الجنائي) من لينكس مشهورة للغاية منذ سنوات. يحتوي Kali على عدد كبير من أدوات التحقيق الجنائي الشائعة التي تستند إلى Linux والتي تتيح لك القيام بكل شيء بدءًا من الفرز الأولي وحتى تصوير البيانات والتحليل الكامل وإدارة الحالات.

❖ **أدوات إعداد التقارير (Reporting Tools):** لا يكتمل اختبار الاختراق إلا بعد الإبلاغ عن النتائج. تحتوي هذه الفئة على أدوات للمساعدة في تجميع البيانات التي تم جمعها من أدوات جمع المعلومات، واكتشاف العلاقات غير الواضحة، والجمع بين كل شيء في تقارير مختلفة.

❖ **أدوات الهندسة الاجتماعية (Social Engineering Tools):** عندما يكون الجانب الفني مضمونًا بشكل جيد من الناحية الدفاعية، غالبًا ما تكون هناك إمكانية لاستغلال السلوك الإنساني كهدف للهجوم. بالنظر إلى التأثير الصحيح، يمكن حث الناس على اتخاذ الإجراءات التي تعرِّض أمن البيئة للخطر. هل يحتوي مفتاح USB الذي وصله السكرتير للتو على ملف PDF غير ضار؟ أم هل كان حصان طروادة أيضًا قام بتثبيت الباب الخلفي؟ هل كان موقع الويب المصرفي هو المحاسب الذي قام للتو بتسجيل الدخول إلى موقع الويب المتوقع أم نسخة كاملة تستخدم لأغراض التصيد؟ تحتوي هذه الفئة على أدوات تساعد في هذه الأنواع من الهجمات.

❖ **خدمات النظام (System Services):** تحتوي هذه الفئة على أدوات تسمح لك ببدء وإيقاف التطبيقات التي تعمل في الخلفية كخدمات للنظام.

4.1. ميزات Kali linux الرئيسية

Kali Linux هي توزيعة Linux تحتوي على مجموعة خاصة من مئات أدوات البرمجيات المصممة خصيصًا للمستخدمين المستهدفين - مختبري الإختراق وغيرهم من متخصصي الأمان-. يأتي أيضًا مع برنامج تثبيت لإعداد Kali Linux بالكامل كنظام تشغيل رئيسي على أي جهاز حاسوب.

يشبه هذا إلى حد كبير جميع توزيعات Linux الأخرى الموجودة، لكن هناك ميزات أخرى تميز Kali Linux، والتي تم تصميم العديد منها لتلبية الاحتياجات المحددة لاختبار الاختراق. دعنا نلقي نظرة على بعض هذه الميزات.

1.4.1. نظام مباشر

على عكس معظم توزيعات Linux، فإن صورة ISO الرئيسية التي تقوم بتنزيلها ليست مخصصة فقط لتثبيت النظام؛ بل يمكنك استخدامها أيضًا كنظام مباشر قابل للإقلاع. بمعنى آخر، يمكنك استخدام Kali Linux دون تثبيته، فقط عن طريق تشغيل صورة ISO (عادةً بعد نسخ الصورة على مفتاح USB).

يحتوي النظام المباشر على الأدوات الأكثر استخداماً في اختبار الاختراق، لذا حتى لو لم يكن نظامك الاساسي هو Kali Linux، يمكنك ببساطة إدخال القرص أو مفتاح USB وإعادة التشغيل لتشغيل Kali. ومع ذلك، ضع في اعتبارك أن التكوين الافتراضي لن يحفظ التغييرات بين عمليات إعادة الإقلاع. إلا إذا قمت بتكوين الثبات باستخدام مفتاح USB (انظر القسم "إضافة الثبات إلى Live ISO باستخدام USB")، يمكنك تعديل النظام حسب رغبتك (تعديل ملفات التهيئة، وحفظ التقارير، وترقية البرامج، وتثبيت حزم إضافية، إلخ ...)، وسيتم الاحتفاظ بالتغييرات حتى بعد إعادة تشغيل الحاسوب.

2.4.1. وضع التحقيق الجنائي

بشكل عام، عند القيام بعمل التحقيق الجنائي على نظام ما، فأنت تريد تجنب أي نشاط من شأنه أن يغير البيانات الموجودة على النظام الذي تم تحليله بأي طريقة. لسوء الحظ، تميل بيئات سطح المكتب الحديثة إلى التداخل مع هذا الهدف من خلال محاولة وصل أي قرص (أقراص) تكتشفها تلقائيًا. لتجنب هذا السلوك، يحتوي Kali Linux على وضع التحقيق الجنائي الذي يمكن تمكينه من قائمة الإقلاع: سيعطل كل هذه الميزات.

يعد النظام المباشر مفيدًا بشكل خاص لأغراض التحقيق الجنائي، لأنه من الممكن إعادة تشغيل أي جهاز حاسوب في نظام Kali Linux دون وصل الأقراص الصلبة أو تعديلها.

3.4.1. تخصيص نواة لينكس

يوفر Kali Linux دائمًا نواة Linux مخصصة حديثًا، استنادًا إلى الإصدار في Debian Unstable. هذا يضمن دعم العتاد (الهاردوير)، وخاصة بالنسبة لمجموعة واسعة من تعريف الأجهزة اللاسلكية. النواة مصححة لدعم الحقن اللاسلكية؛ لأن بعض أدوات تقييم الأمان اللاسلكية تعتمد على هذه الميزة.

نظرًا لأن العديد من الأجهزة تتطلب ملفات برامج ثابتة محدثة (موجودة في /lib/firmware/)، فإن Kali تقوم بتثبيتها جميعًا بشكل افتراضي - بما في ذلك البرامج الثابتة المتوفرة في القسم الغير مجاني في Debian. لم يتم تثبيتها افتراضياً في Debian، لأنها مصدر مغلق وبالتالي فهي ليست جزءًا من Debian.

4.4.1. تخصيص بكل معنى الكلمة

تم تصميم Kali Linux من قِبل مختبري اختراق وهو لمختبري الاختراق، لكننا نتفهم أنه لن يوافق الجميع على قرارات التصميم الخاصة بنا أو اختيار الأدوات التي يجب تضمينها افتراضياً. مع وضع ذلك في الاعتبار، نحن نضمن دائمًا سهولة تخصيص Kali Linux حسب احتياجاتك وتفضيلاتك. تحقيقًا لهذه الغاية، ننشر تهيئة البناء المباشر المستخدمة في إنشاء صور Kali الرسمية حتى تتمكن من تخصيصها حسب رغبتك. من السهل جدًا البدء في هذا التكوين وتنفيذ تغييرات متنوعة بناءً على احتياجاتك بفضل براعة Live-build.

يتضمن Live-build العديد من الميزات لتعديل النظام المثبت، وتثبيت الملفات الإضافية، وتثبيت حزم إضافية، وتشغيل الأوامر التعسفية (arbitrary commamds)، وتغيير القيم التي تم نقلها مسبقًا إلى debconf.

5.4.1. نظام تشغيل موثوق

يجب على المستخدمين الأمنيين معرفة أنه يمكنهم الوثوق به لأنه تم تطويره في مرأى من الجميع ولأنه يمكن لأي شخص فحص الكود المصدري. تم تطوير Kali Linux بواسطة فريق صغير من المطورين ذوي المعرفة، يعملون بشفافية ويتبعون أفضل ممارسات الأمان: يقومون بتحميل حزم المصدر الموقعة والتي يتم بناؤها بعد ذلك، يتم اختبار الحزم وتوزيعها كجزء من حزم الموقع.

يمكن مراجعة العمل المنجز على الحزم بالكامل من خلال حزم Git للتعبئة والتغليف (التي تحتوي على علامات موقعة) والتي يتم استخدامها لإنشاء حزم مصادر Kali. يمكن أيضًا متابعة تطور كل حزمة من خلال حزم Kali Tracker.

6.4.1. قابلة للاستخدام على مجموعة واسعة من أجهزة ARM

يوفر Kali Linux حزمًا ثنائيةً لبُنْيَات armel و armhf و arm64 ARM. بفضل الصور القابلة للتثبيت بسهولة والتي يوفرها Offensive Security، يمكن نشر Kali Linux على العديد من الأجهزة المثيرة للاهتمام، من الهواتف الذكية والأجهزة اللوحية إلى أجهزة توجيه (Router) Wi-Fi وأجهزة الحاسوب من مختلف الأشكال والأحجام.

5.1. سياسات Kali Linux

بينما تسعى Kali Linux جاهدة إلى اتباع سياسة Debian كلما أمكن ذلك، هناك بعض المجالات التي اتخذنا فيها خيارات تصميم مختلفة إلى حد كبير بسبب الاحتياجات الخاصة لمتخصصي الأمن.

1.5.1. مستخدم جذر واحد افتراضيًا

(*لن يكون هذا مع بداية ٢٠٢٠*) تشجع معظم توزيعات Linux، بشكل معقول، استخدام حساب غير متميز أثناء تشغيل النظام واستخدام أداة مساعدة مثل **sudo** عند الحاجة إلى امتيازات إدارية. هذه نصيحة أمنية سليمة، توفر طبقة إضافية من الحماية بين المستخدم وأي أوامر أو عمليات لنظام تشغيل تحتمل التخريب أو التدمير. ينطبق هذا بشكل خاص على أنظمة المستخدم المتعددة، حيث يكون الفصل بين امتياز المستخدم متطلباً — فقد يؤدي سوء تصرف أحد المستخدمين إلى تعطيل عمل العديد من المستخدمين أو إتلاف حساباتهم أو إتلاف النظام.

نظراً لأن العديد من الأدوات المضمنة في Kali Linux لا يمكن تنفيذها إلا بامتيازات الجذر، فهذا هو حساب مستخدم Kali الافتراضي. بخلاف توزيعات Linux الأخرى، لن تتم مطالبتك بإنشاء مستخدم غير متميز عند تثبيت Kali. تمثل هذه السياسة بالذات انحرافاً كبيراً عن معظم أنظمة Linux وتميل إلى أن تكون مربكة للغاية للمستخدمين الأقل خبرة. يجب على المبتدئين توخي الحذر بشكل خاص عند استخدام Kali لأن معظم الأخطاء المدمرة تحدث عند العمل بامتيازات الجذر.

2.5.1. تم تعطيل خدمات الشبكة بشكل افتراضي

على عكس Debian، يقوم Kali Linux بتعطيل أي خدمة مثبتة تستمع على واجهة شبكة عامة بشكل افتراضي، مثل: HTTP وSSH.

الأساس المنطقي وراء هذا القرار هو تقليل التعرض أثناء اختبار الاختراق عندما يكون من الضار الإعلان عن وجودك والكشف عن المخاطر بسبب تفاعلات الشبكة غير المتوقعة.

لا يزال بإمكانك تمكين أي خدمة عن طريق كتابة الأمر:

```
systemctl enable service
```

سنناقش هذا في الفصل الخامس، تكوين Kali Linux.

3.5.1. مجموعة تطبيقات مختارة

تهدف Debian إلى أن تكون نظام التشغيل العالمي وتضع قيودًا قليلة جدًا على ما يتم تعبئته، شريطة أن يكون لكل حزمة صيانة.

على النقيض من ذلك، لا يقوم Kali Linux بحزم كل أداة لاختبار الاختراق المتاحة. بدلاً من ذلك، نهدف إلى توفير أفضل الأدوات المرخصة بحرية والتي تغطي معظم المهام التي قد يرغب مختبر الاختراق في تنفيذها.

يعمل مطورو Kali الذين يعملون كمختبرين للاختراق على التحكم في عملية الاختيار، ونستفيد من تجاربهم وخبراتهم في اتخاذ خيارات صحيحة.

فيما يلي بعض النقاط التي يتم أخذها في الاعتبار عند تقديم طلب جديد:

- ❖ فائدة التطبيق في مجال اختبار الاختراق
- ❖ الوظيفة الفريدة لميزات التطبيق
- ❖ رخصة التطبيق
- ❖ متطلبات موارد التطبيق

يعد الاحتفاظ بحزم أدوات اختبار الاختراق المحدثة والمفيدة مهمة صعبة. نرحب باقتراحات الأدوات ضمن فئة مخصصة (New Tool Requests) في Kali Bug Tracker. يتم تلقي طلبات الأداة الجديدة على أفضل وجه عندما يتم تقديم المقترح جيدًا، بما في ذلك شرح لمدى فائدة الأداة وكيف تقارن بالتطبيقات الأخرى المشابهة وما إلى ذلك.

6.1. ملخص

في هذا الفصل قدمنا لك Kali Linux، قدمنا نبذة عن تاريخه، وعلى بعض الميزات الأساسية، وحالات الاستخدام. لقد ناقشنا أيضًا بعض السياسات التي اعتمدناها عند تطوير Kali Linux.

نصائح التلخيص:

- ❖ Kali Linux هي توزيعة Linux جاهزة لمراجعة حسابات الشركات، وتستند على Debian GNU / Linux. يهدف Kali إلى المتخصصين في مجال الأمن ومسؤولي تقنية المعلومات، مما يمكنهم من إجراء اختبارات الاختراق المتقدمة والتحقيق الجنائي وتدقيق الأمان.
- ❖ على عكس معظم أنظمة التشغيل الرئيسية، يعد Kali Linux توزيعًا مستمرًا، مما يعني أنك ستتلقى التحديثات كل يوم.
- ❖ تستند توزيعة Kali Linux على Debian testing. لذلك، تأتي معظم الحزم المتوفرة في Kali Linux مباشرة من مستودع Debian هذا.
- ❖ بينما يمكن تلخيص استخدام Kali بسرعة بـ "اختبار الاختراق ومراجعة الأمان"، هناك العديد من حالات الاستخدام، بما في ذلك مسؤولو النظام الذين يرغبون في مراقبة شبكاتهم، وعمل التحقيق الجنائي، وتركيبات الأجهزة المدمجة، والمراقبة اللاسلكية، والتثبيت على المنصات المحمولة، وأكثر من ذلك.
- ❖ تسهل قوائم Kali الوصول إلى الأدوات الخاصة بالمهام والأنشطة المختلفة بما في ذلك: تحليل الثغرات الأمنية، وتحليل تطبيقات الويب، تقييم قواعد البيانات، هجمات كلمة المرور، الهجمات اللاسلكية، الهندسة العكسية، أدوات الاستغلال، الشم والخداع، أدوات ما

بعد الاستغلال، التحقيق الجنائي، أدوات إعداد التقارير، وأدوات الهندسة الاجتماعية، وخدمات النظام.

❖ يحتوي Kali Linux على العديد من الميزات المتقدمة بما في ذلك: الاستخدام كنظام مباشر (غير مثبت)، ووضع التحقيق الجنائي القوي والآمن، ونواة Linux مخصصة، والقدرة على تخصيص النظام بالكامل، ونظام تشغيل أساسي موثوق به وآمن، وإمكانية تثبيت ARM، وسياسات الشبكة الافتراضية الآمنة، ومجموعة من التطبيقات المختارة.

في الفصل التالي، سنبدأ مع بعض أساسيات Linux.

التمرين الأول، الفصل الأول - إعداد بيئتنا

١. قم بإنشاء VM جديد في VMware (اختار Debian 64 bit).
٢. قم بتعيينه على الأقل من ذاكرة الوصول العشوائي (RAM) سعة 2 GB، وحدتي CPU، و 30 GB للقرص الصلب
٣. ربط صورة ISO Kali إلى CDROM الإفتراضي.
٤. تأكد من أن VM في وضع NAT.
٥. قم بتشغيل جهاز VM، وفحص خيارات الإقلاع Kali وفهمها.

غذاء الفكر

١. ما هو إصدار ديبيان Debian التي يستند عليه Kali 1.0 و Rolling 2.0؟
٢. ما هي الاختلافات الرئيسية بين الإقلاع المباشر لـ Kali والمثبت؟
٣. ما الفرق بين وضع الإقلاع المباشر ووضع التحقيق الجنائي؟
٤. كيف يمكننا التحقق من أن وضع التحقيق الجنائي يعمل؟
٥. ما هي أفضل طريقة لإدراج أداة في Kali؟
٦. اسم بعض الميزات الرائعة في Kali؟

الإجابات

تحقق من كل خيارات الإقلاع. استخدم "tap" لتحرير معلمات الإقلاع في حالة استخدام syslinux أو "e" إذا كنت تستخدم grub.



١. المباشر – الإقلاع المباشر، كالمعتاد.

٢. المباشر (الوضع الآمن) – يقلع بأقل تعريفات للهاردوير والأجهزة. // الأجهزة المطلوبة فقط//

٣. المباشر (التحقيق الجنائي) - يقلع دون وصل أي شيء، ومناسبة لعمل التحقيق الجنائي.

٤. مباشر (ثابت ومشفر) - ما عليك سوى إضافة الأقسام المطلوبة، وقائمة الإقلاع جاهزة للاستمرار.

٥. تثبيت (install) - عادي، بواجهة قديمة

٦. تثبيت رسومي - وضع التثبيت بواجهة المستخدم الرسومية الخاصة بنظام كالي

٧. التثبيت بالنطق - تثبيت Kali للمستخدمين ضعاف البصر.

٨. أداة الكشف عن الأجهزة - مصممة لعرض معلومات الأجهزة ذات المستوى المنخفض.

٩. تشخيص الذاكرة - erm، تشخيص الذاكرة!

إجابات غذاء الفكر

١. يستند Kali 1.0 على Debian Wheezy، بينما Kali 2.0 يستند على Jessie.

٢. يتم تشغيل الوضع المباشر على ذاكرة الوصول العشوائي (RAM) وKali المثبت على ذاكرة تخزين.

٣. يتم تشغيل الوضع المباشر على ذاكرة الوصول العشوائي، ولكن قد يتم تحميل الأقراص تلقائيًا. وضع التحقيق الجنائي لا يقوم بوصل محركات الأقراص تلقائيًا.

٤. استخدم الأمر **mount** للتحقق من عدم تركيب أي أقراص. يمكنك أيضًا استخراج هاش md5 وتبديل النظام وأجهزة الأقراص، وإعادة التشغيل في وضع التحقيق الجنائي واستخراج هاش md5 مرة أخرى. يجب أن يتطابقا الهاشا الـ md5 إذا نجح وضع التحقيق الجنائي. جرب هذا في نظام لا يهمك أن يتغير ما فيه!

٥. أفضل طريقة لطلب إضافة أداة هي فتح تذكرة "New Tool Requests" في Kali Bug Tracker.

٦. نظام مباشر، وضع التحقيق المباشر، نواة لينكس مخصصة، قابلة للتخصيص بالكامل، نظام تشغيل موثوق به مع خدمات الشبكة الافتراضية المعطلة، دعم ARM، أدوات الأمان المحملة مسبقًا، منصة اختبار الاختراق!

اختبار KLCP الاختبار الأول

ما هو أحدث إصدار من Kali:

- ○ توزيع ثابت، يستند على Debian testing Wheezy.
- ○ توزيع ثابت، يستند على Debian Stable Jessie.
- ○ توزيع مستمر، يستند على Debian testing.
- ○ توزيع مستمر، يستند على Debian Stable Wheezy.

الإجابة:

توزيع مستمر، يستند على Debian testing.

A rolling distribution based on Debian testing

---((الفصل الثاني))---

2. البداية مع Kali

على عكس بعض أنظمة التشغيل الأخرى، فإن Kali Linux يجعل البداية سهلة، بفضل حقيقة أن صوره على القرص هي ISOs مباشرة، مما يعني أنه يمكنك تشغيل الصورة التي تم تنزيلها دون اتباع أي إجراء تثبيت مسبق. هذا يعني أنه يمكنك استخدام نفس الصورة للاختبار أو لاستخدامها كصورة USB أو DVD-ROM قابلة للإقلاع في حالة التحقيق الجنائي أو للتثبيت كنظام تشغيل أساسي على أجهزة حقيقية أو افتراضية.

مع هذه البساطة، يجب ألاَّ ننسى أنه يجب اتخاذ بعض الاحتياطات. غالبًا ما يكون مستخدمو Kali هدفًا للذين عندهم نوايا سيئة، سواءً كانت مجموعات تمولها الدول أو عناصر من الجريمة المنظمة أو مخترقين فرديين. بسبب طبيعة Kali Linux (المفتوحة المصدر) من السهل نسبيًا إنشاء إصدارات مزيفة وتوزيعها؛ لذلك من الضروري أن تتعرف على عملية التنزيل من المصادر الأصلية والتحقق من سلامة صورتك التي قمت بتنزيلها. هذا مهم بشكل خاص لمتخصصي الأمن الذين غالبًا ما يمكنهم الوصول إلى الشبكات الحساسة والمكلفين ببيانات العميل.

1.2. تنزيل صورة ISO لنظام كالي

1.1.2. من أين يمكنني الحصول على نظام كالي

المصدر الرسمي الوحيد لصور Kali Linux ISO هو قسم "Downloads" في موقع Kali الإلكتروني.

https://www.kali.org/downloads/

نظراً لشهرته، تقدم العديد من المواقع صور Kali للتنزيل، لكن لا ينبغي اعتبارها جديرة بالثقة قد تكون مصابة بالفعل ببرامج ضارة أو تتسبب في ضرر لا يمكن إصلاحه لنظامك.

الموقع متاح عبر HTTPS، مما يجعل من الصعب انتحال شخصيته. لا تكون القدرة على تنفيذ هجوم رجل في الوسط كافية، لأن المهاجم سيحتاج أيضًا إلى شهادة www.kali.org موقعة من سلطة شهادة أمن طبقة النقل "Transport Layer Security" (TLS) موثوق بها من قبل متصفح الضحية. نظراً لوجود سلطات الشهادات على وجه التحديد لمنع هذا النوع من المشكلات، فإنها تقدم شهادات فقط للأشخاص الذين تم التحقق من هويتهم والذين قدموا أدلة على أنهم يتحكمون في موقع الويب المقابل.

cdimage.kali.org

تشير الارتباطات الموجودة على صفحة التنزيل إلى مجال (Domain) **cdimage.kali.org**، الذي يعيد توجيهك لمرآة قريبة منك، مما يحسن سرعة النقل مع تقليل العبء على خوادم Kali المركزية.يمكن الاطلاع على قائمة بالمرايا المتوفرة هنا: http://cdimage.kali.org/README.mirrorlist

٢.١.٢. ماذا يوجد في قسم "Downloads"

تعرض صفحة التنزيل الرسمية قائمة قصيرة من صور ISO، كما هو مبين في الشكل ٢.١. "قائمة الصور المعروضة للتنزيل".

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to **download Kali Linux** in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/.

Image Name	Download	Size	Version	sha256sum
Kali 64 bit	ISO | Torrent	2.9G	2016.2	1d90432e6d5c6f40dfe9589d9d0450a53b0add9a55f71371d601a5d454fa0431
Kali 32 bit	ISO | Torrent	2.9G	2016.2	c94772c4fd71f50b245c7b15f4f225ad7c751879f501fa1cf698beb1460c0bf5
Kali 64 bit Light	ISO | Torrent	1.1G	2016.2	997f5ed0f7c99c4518288c7e2c4b684b1bdcc2fbe02c152d7ecbd17f0536c29f
Kali 32 bit Light	ISO | Torrent	1.1G	2016.2	590e6df2e8e0b4d42bf3dd4e4c7d6acf24b7262fabda52a0c6c3b35006def295
Kali 64 bit e17	ISO | Torrent	2.7G	2016.2	404d0fd917a404cf6c894b5bd87171ebf8eb445bd5573a3e78f88629067d694b
Kali 64 bit Mate	ISO | Torrent	2.8G	2016.2	cd11b7085cc7d71546488106c2eedf85386fe73d731bedf38991661270dd91db
Kali 64 bit Xfce	ISO | Torrent	2.7G	2016.2	3e08e5420b368183606b105cf2cb1276dd024afe3e2b2e3187d7d37ec1320c41
Kali 64 bit LXDE	ISO | Torrent	2.7G	2016.2	7461882843e5a0fc37979850994fb5755249a176429f9e67805bd7f6baa5bb62
Kali armhf	Image | Torrent	0.7G	2016.2	f192289b6bc64bab7197a90627ced2477c7c98bd20c1d29f442a152e169dae42
Kali armel	Image | Torrent	0.7G	2016.2	efb6f487feab1c9141f28da22c73cbc5217325bf46298f899ac89c39c19aa5f5

شكل ٢.١. قائمة الصور المعروضة للتنزيل

تشير جميع صور الأقراص المسمى 32 أو 64 بت إلى الصور المناسبة لوحدات المعالجة المركزية، الموجودة في معظم أجهزة الحاسوب المكتبية والحاسوب المحمول الحديث. إذا كنت تقوم بالتنزيل للاستخدام على جهاز حديث إلى حد ما، فمن المحتمل أنه يحتوي على معالج 64 bit. إذا لم تكن متأكدًا، فكن على يقين من أن جميع معالجات 64 bit يمكنها تشغيل 32 bit. يمكنك دائمًا تنزيل وتشغيل صورة 32 bit. والعكس ليس صحيحًا.

إذا كنت تخطط لتثبيت Kali على جهاز مضمن أو هاتف ذكي أو Chromebook أو نقطة وصول أو أي جهاز آخر باستخدام معالج ARM، فيجب عليك استخدام Linux armel أو صور armhf.

هل معالجي 32 أو 64 بت؟

في **Windows**، يمكنك العثور على هذه المعلومات عن طريق تشغيل تطبيق "معلومات النظام" (الموجود في مجلد "البرامج الملحقة"> "أدوات النظام"). على شاشة ملخص النظام، يمكنك فحص حقل "نوع النظام": سوف يحتوي على "حاسوب يستند إلى x64" لوحدة المعالجة المركزية 64 bit أو "حاسوب يستند إلى x86" لوحدة المعالجة المركزية 32 bit.

في **OS X / macOS**، لا يوجد تطبيق قياسي يعرض هذه المعلومات ولكن لا يزال بإمكانك استنتاجها من مخرجات الأمر **uname -m** الذي يتم تشغيله على الـ terminal. سيرجع x86_64 لنظام يحتوي على نواة 64 bit (والذي لا يمكن تشغيله إلا على وحدة المعالجة المركزية 64 bit) وعلى الأنظمة التي تحتوي على نواة 32 bit، سيرجع i386 أو شيء مشابه (i486 أو i586 أو i686). يمكن تشغيل أي نواة 32 bit على وحدة المعالجة المركزية 64 bit، ولكن بما أن Apple تتحكم في الأجهزة والبرامج، فمن غير المرجح أن تجد هذا التكوين.

في **Linux**، يمكنك التحقق من حقل flags في الملف الافتراضي proc/cpuinfo/. إذا كانت تحتوي على lm، فإن وحدة المعالجة المركزية لديك هي 64 bit؛ غير ذلك، يعني 32 bit. سيخبرك سطر الأوامر التالي بنوع وحدة المعالجة المركزية لديك:

```
grep -qP '^flags\s*:.*\blm\b' /proc/cpuinfo && echo 64-bit || echo 32-bit
64-bit
```

الآن بعد أن عرفت ما إذا كنت تحتاج إلى صورة 32 bit أو 64 bit، هناك فقط خطوة واحدة متبقية: تحديد نوع الصورة. تعد صورة Kali Linux الافتراضية و Kali Linux Light كلاهما من ISOs المباشرة التي يمكن استخدامها لتشغيل النظام المباشر أو لبدء عملية التثبيت. أنها تختلف في مجموعة التطبيقات المثبتة مسبقا. تأتي الصورة الافتراضية مع سطح مكتب Gnome ومجموعة كبيرة من الحزم التي وجد أنها مناسبة لمعظم اختبارات الاختراق، في حين تأتي الصورة الخفيفة مع سطح مكتب XFCE (الذي هو أقل طلباً على موارد النظام)، ومجموعة محدودة من الحزم، مما يسمح لك باختيار التطبيقات التي تحتاجها فقط. تستخدم الصور الأخرى بيئات سطح مكتب مختلفة ولكنها تأتي بنفس المجموعة الكبيرة الحجم مثل الصورة الرئيسية.

بمجرد أن تقرر الصورة التي تحتاجها، يمكنك تنزيل الصورة من خلال النقر على "ISO" في الصف المخصص. أو يمكنك تنزيل الصورة من شبكة BitTorrent الند للند من خلال النقر على "Torrent"، شريطة أن يكون لديك عميل BitTorrent مرتبط بامتدادtorrent..

أثناء تنزيل صورة ISO التي اخترتها، يجب أن تأخذ ملاحظة المجموع الاختباري المكتوب في عمود "sha256sum". بمجرد تنزيل صورتك، ستستخدم هذا المجموع الاختباري للتحقق من أن الصورة التي تم تنزيلها تتطابق مع الصورة التي وضعها مطورو Kali عبر الإنترنت (انظر القسم التالي).

٢.١.٣. التحقق من النزاهة والأصالة

يجب على محترفي الأمان التحقق من سلامة أدواتهم ليس فقط لحماية بياناتهم وشبكاتهم ولكن أيضًا لعملائهم. بينما تكون صفحة تنزيل Kali محمية بواسطة TLS، يشير رابط التنزيل الفعلي إلى عنوان URL غير مشفر لا يوفر أي حماية ضد هجمات man-in-the-middle المحتملة. حقيقة أن كالي تعتمد على شبكة من المرايا الخارجية لتوزيع الصورة يعني أنك يجب ألا تثق ثقة عمياء بما تقوم بتنزيله. قد تكون المرآة التي تم توجيهك إليها قد تعرضت للاختراق، أو قد تكون ضحية لهجوم بنفسك.

للتخفيف من ذلك، يوفر مشروع Kali دائمًا مقاطع اختبارية للصور التي يوزعها. ولكن لجعل هذا الفحص فعالًا، يجب أن تكون على يقين من أن المجموع الاختباري الذي استخرجته هو المجموع الاختباري الذي نشره مطورو Kali Linux. لديك طرق مختلفة للتأكد من هذا.

٢.١.٣.١. الاعتماد على موقع TLS المحمي

عندما تسترجع المجموع الاختباري من صفحة الويب للتنزيل المحمي بـ TLS، فإن أصلها مضمون بشكل غير مباشر بواسطة نموذج أمان شهادة X.509: المحتوى الذي تراه يأتي من موقع ويب يخضع فعلياً لسيطرة الشخص الذي طلب شهادة TLS.

الآن يجب عليك إنشاء المجموع الاختباري لصورتك التي تم تنزيلها والتأكد من مطابقتها لما قمت بتسجيله من موقع Kali:

```
$ sha256sum kali-linux-2016.2-amd64.iso
1d90432e6d5c6f40dfe9589d9d0450a53b0add9a55f71371d601a5d454fa0431
kali-linux-2016.2-amd64.iso
```

إذا تطابق المجموع الاختباري الذي تم إنشاؤه مع الموجود في صفحة تنزيل Kali Linux، فلديك الملف الصحيح. في حالة اختلاف النتائج، هناك مشكلة، رغم أن هذا لا يشير إلى حل وسط أو هجوم؛ التنزيلات تتلف أحيانًا لأنها تجتاز الإنترنت. جرب التنزيل مرة أخرى، من مرآة Kali الرسمية الأخرى، إن أمكن (انظر cdimage.kali.org لمزيد من المعلومات حول المرايا المتوفرة).

٢.٣.١.٢. الاعتماد على شبكة PGP الخاصة بالثقة

إذا كنت لا تثق في HTTPS للمصادقة، فعندك جنون العظمة قليلاً ولكن معك حق. هناك العديد من الأمثلة لسلطات الشهادات التي تتم إدارتها بشكل سيء والتي أصدرت شهادات فاسدة، والتي انتهى الأمر بإساءة استخدامها. قد تكون أيضًا ضحية هجوم man-in-the-middle "الودي" الذي يتم تنفيذه على العديد من شبكات الشركات، وذلك باستخدام متجر ثقة مخصص مزروع بواسطة المستعرض يقدم شهادات مزيفة لجميع مواقع الويب المشفرة SSL، مما يسمح لمراجعي الشركات بمراقبة حركة المرور المشفرة.

في حالات كهذه، نوفر أيضًا مفتاح GnuPG الذي نستخدمه للتوقيع على اختبار الصور التي نقدمها. معرّفات المفتاح والبصمات معروضة هنا:

```
pub   4096R/7D8D0BF6 2012-03-05 [expires: 2018-02-02]
Key fingerprint = 44C6 513A 8E4F B3D3 0875  F758
ED44 4FF0 7D8D 0BF6
uid  Kali Linux Repository devel@kali.org
sub   4096R/FC0D0DCB 2012-03-05 [expires: 2018-02-02]
```

هذا المفتاح جزء من شبكة ثقة عالمية لأنه تم توقيعه على الأقل من قبلي (Raphaël Hertzog) وأنا جزء من شبكة الثقة بسبب استخدامي المكثف لـ GnuPG كمطور لديبيان.

طراز الأمان PGP / GPG فريد من نوعه. يمكن لأي شخص إنشاء أي مفتاح له أي هوية، لكنك لن تثق بهذا المفتاح إلا إذا تم توقيعه بواسطة مفتاح آخر تثق به بالفعل. عندما تقوم بالتوقيع على مفتاح، فإنك تقر بأنك قابلت حامل المفتاح وأنك تعلم أن الهوية المرتبطة صحيحة. ويمكنك تحديد المجموعة الأولية من المفاتيح التي تثق بها، والتي تتضمن بوضوح مفتاحك الخاص.

هذا النموذج له حدوده الخاصة، لذا يمكنك اختيار تنزيل مفتاح Kali العام عبر HTTPS (أو من خادم مفاتيح) وقرر فقط أن تثق به لأن بصمة أصبعه تتطابق مع ما أعلناه في أماكن متعددة، بما في ذلك أعلاه فقط في هذا الكتاب:

```
$ wget -q -O - https://www.kali.org/archive-key.asc
| gpg --import
[ or ]
$ gpg --keyserver hkp://keys.gnupg.net --recv-key
7D8D0BF6
gpg: key 7D8D0BF6: public key "Kali Linux
Repository <devel@kali.org>" imported
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
[...]
$ gpg --fingerprint 7D8D0BF6
[...]
Key fingerprint = 44C6 513A 8E4F B3D3 0875  F758
ED44 4FF0 7D8D 0BF6
[...]
```

الآن وقد حصلنا على المفتاح، يمكننا استخدامه للتحقق من المجموع الاختباري لصور التوزيعة. لنقم بتنزيل الملف باستخدام المجموع الاختباري (SHA256SUMS) وملف التوقيع المقترن (SHA256SUMS.gpg) والتحقق من التوقيع:

```
$wget http://cdimage.kali.org/current/SHA256SUMS
[...]
$wget http://cdimage.kali.org/current/SHA256SUMS.gpg
[...]
$gpg --verify SHA256SUMS.gpg SHA256SUMS
gpg: Signature made Thu 16 Mar 2017 08:55:45 AM MDT
gpg: using RSA key ED444FF07D8D0BF6
gpg: Good signature from "Kali Linux Repository <devel@kali.org>"
```

إذا تلقيت رسالة "توقيع جيد (Good signature)"، فيمكنك الوثوق في محتوى ملف SHA256SUMS واستخدامه للتحقق من الملفات التي قمت بتنزيلها. غير ذلك، هناك مشكلة. يجب عليك مراجعة ما إذا كنت قد قمت بتنزيل الملفات من مرآة Kali Linux شرعية. (قانونية أو معتمدة)

لاحظ أنه يمكنك استخدام سطر الأوامر التالي للتحقق من أن الملف الذي تم تنزيله له نفس المجموع الاختباري المدرج في SHA256SUMS، شريطة أن يكون ملف ISO الذي تم تنزيله في نفس المجلد:

```
$ grep kali-linux-2016.2-amd64.iso SHA256SUMS | sha256sum -c
kali-linux-2016.2-amd64.iso: OK
```

إذا لم تحصل على موافقة "OK"، فالملف الذي قمت بتنزيله يختلف عن الملف الذي أصدره فريق Kali. لا يمكن الوثوق بها ويجب عدم استخدامها.

٤.١.٢. نسخ الصورة على قرص DVD-ROM أو مفتاح USB

ما لم ترغب في تشغيل Kali Linux في جهاز افتراضي، فإن صورة ISO تكون محدودة الاستخدام بحد ذاتها. يجب عليك نسخها على قرص DVD-ROM أو نسخها على مفتاح USB لتتمكن من تشغيل جهازك بنظام Kali Linux.

لن نغطي كيفية نسخ صورة ISO على قرص DVD-ROM، حيث تختلف العملية اختلافًا كبيرًا حسب النظام الأساسي والبيئة، ولكن في معظم الحالات، يؤدي النقر بزر الماوس الأيمن على ملف iso. إلى ستجد في القائمة برنامج حرق DVD- ROM. جرب!

> في هذا القسم، ستتعلم كيفية الكتابة فوق قرص باستخدام صورة Kali Linux ISO. تحقق دائمًا من فحص القرص المستهدف قبل بدء العملية، حيث من المحتمل أن يتسبب خطأ واحد في فقد البيانات بشكل كامل وقد يتسبب في تلف الإعداد (setup) الخاص بك بشكل لا يمكن إصلاحه.

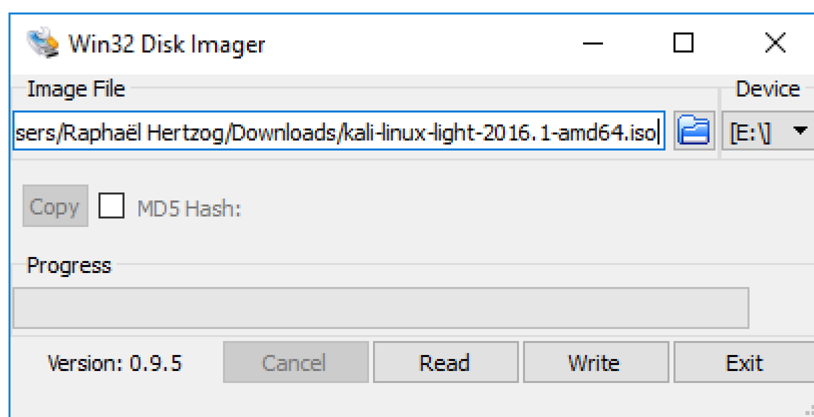
١.٤.١.٢. إنشاء محرك USB كالي قابل للتشغيل على Windows

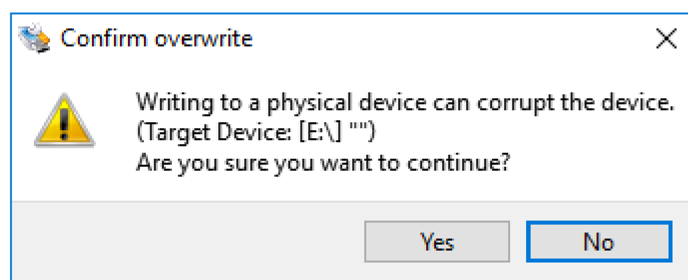
كشرط أساسي، يجب عليك تنزيل وتثبيت Win32 Disk Imager:

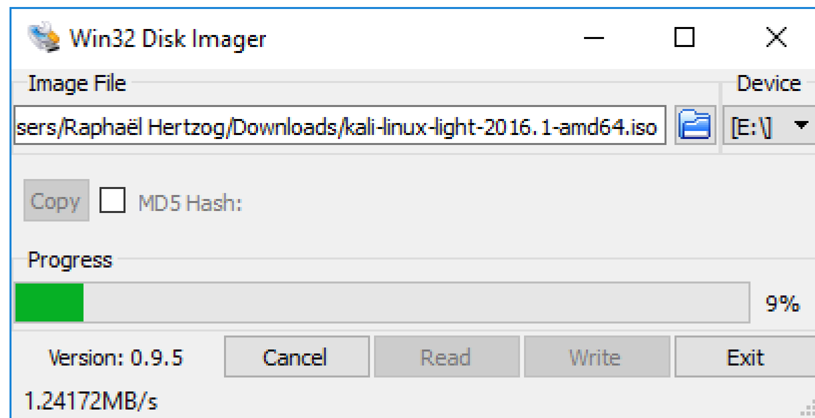
https://sourceforge.net/projects/win32diskimager/

قم بتوصيل مفتاح USB بجهاز الحاسوب الشخصي الخاص بك الذي يعمل بنظام Windows ولاحظ محدد محرك الأقراص المرتبط به (على سبيل المثال، "E:").

قم بتشغيل Win32 Disk Imager واختر ملف Kali Linux ISO الذي تريد نسخه على مفتاح USB. تحقق من أن حرف الجهاز المحدد يتوافق مع ذلك المعين لمفتاح USB. بمجرد التأكد من تحديد محرك الأقراص الصحيح، انقر فوق زر "Write" وتأكد من أنك تريد الكتابة فوق محتويات مفتاح USB كما هو موضح في "شكل 2.2. عملية الكتابة ببرنامج Win32 Disk imager".





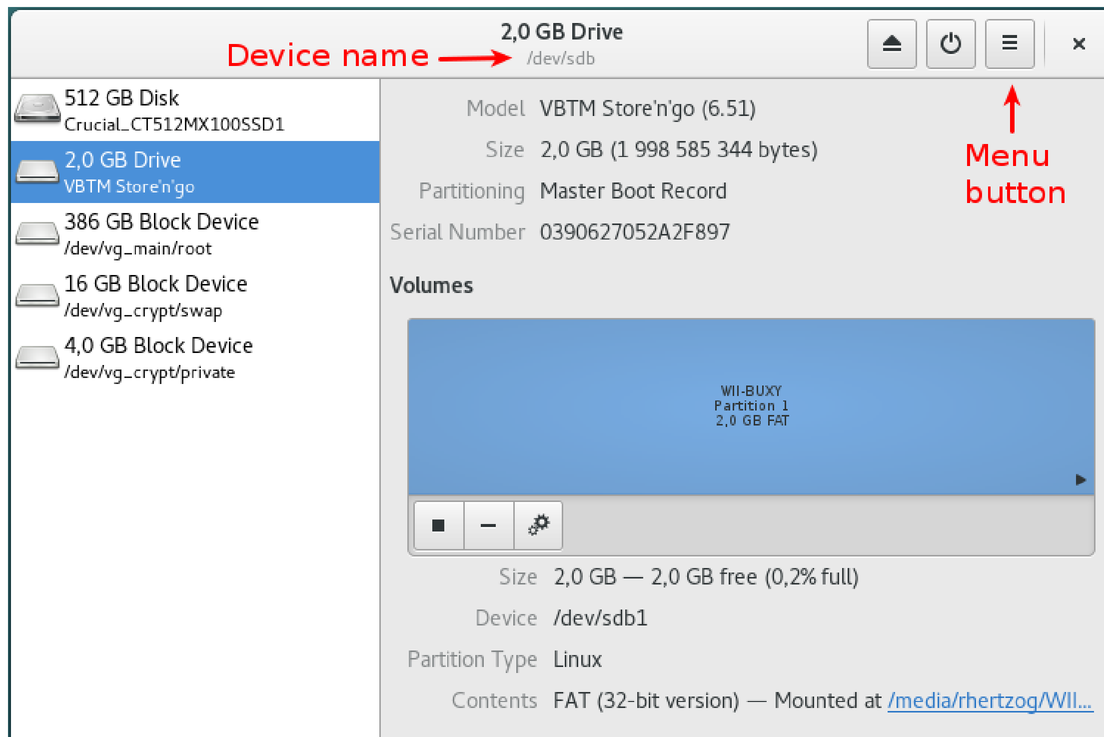


شكل 2.2. عملية الكتابة ببرنامج Win32 Disk imager

بمجرد اكتمال النسخ، أخرج محرك USB بأمان من نظام Windows. يمكنك الآن استخدام جهاز USB لتشغيل Kali Linux.

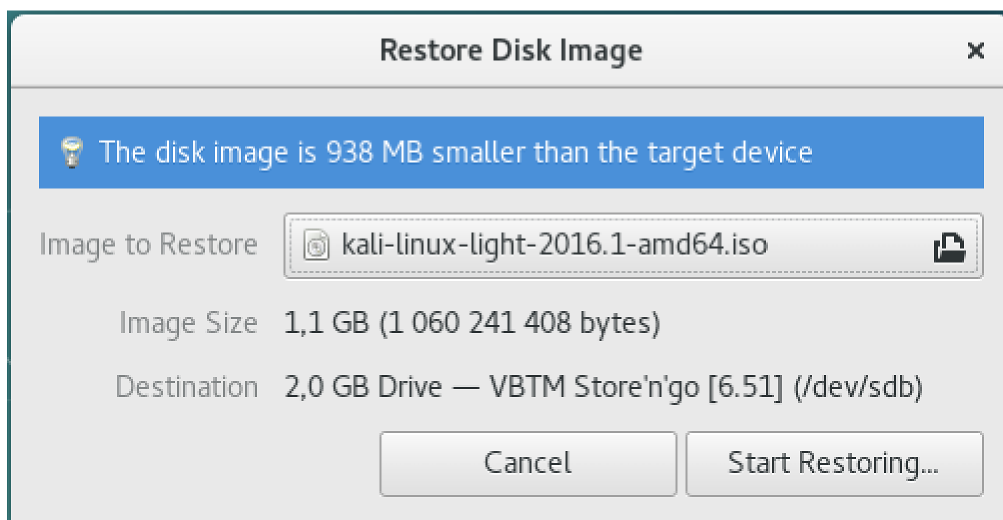
٢.٤.١.٢. إنشاء محرك أقراص USB قابل للإقلاع على نظام Linux

من السهل إنشاء مفتاح Kali Linux USB قابل للإقلاع في بيئة Linux. تأتي بيئة سطح مكتب GNOME، والتي يتم تثبيتها افتراضياً في العديد من توزيعات Linux، مع أداة (Disks utility) (في حزمة الأداة المساعدة gnome-disk-tool، والتي تم تثبيتها بالفعل في صورة Kali). يعرض هذا البرنامج قائمة بالأقراص، والتي يتم تحديثها بشكل مستمر عند توصيل قرص أو فصله. عند تحديد مفتاح USB الخاص بك في قائمة الأقراص، ستظهر معلومات مفصلة وسوف تساعدك على تأكيد تحديد القرص الصحيح. لاحظ أنه يمكنك العثور على اسم الجهاز الخاص به ((أو مسار الجهاز لأن كل شيء في لينكس عبارة عن ملفات)) في شريط العنوان كما هو موضح في الشكل ٣.٢، "GNOME Disks".



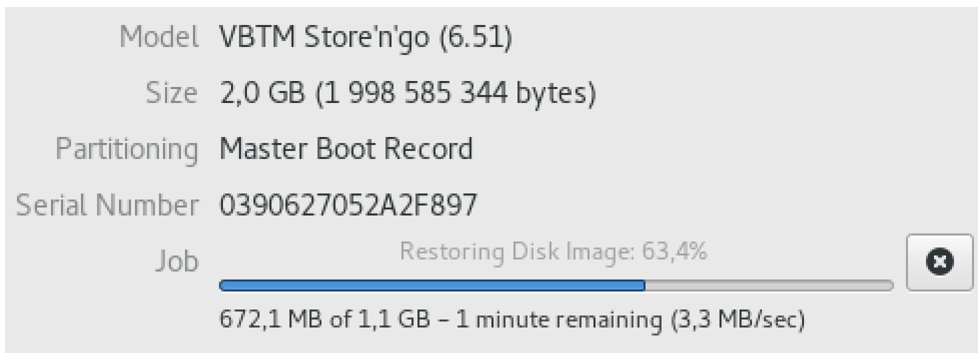
شكل ٣.٢. GNOME Disks

انقر على زر القائمة واختار Restore Disk Image... في القائمة المنبثقة المعروضة. حدد صورة ISO التي قمت بتنزيلها مسبقًا وانقر فوق "Start Restoring..." كما هو موضح في الشكل ٤.٢. "Restore Disk Image Dialog".



شكل ٤.٢. "Restore Disk Image Dialog"

استمتع بفنجان من القهوة بينما تنتهي من نسخ الصورة على مفتاح USB شكل) 2.5 “Progression of the Image Restoration).



شكل ٥.٢. Progression of the Image Restoration

إنشاء محرك أقراص USB قابل للإقلاع من سطر الأوامر

على الرغم من أن العملية الرسومية واضحة إلى حد ما، إلا أن العملية سهلة لمستخدمي سطر الأوامر.

عندما تقوم بإدخال مفتاح USB الخاص بك، فإن نواة Linux ستكتشفه وتعين له اسمًا، وهو مطبوع في سجلات النواة. يمكنك العثور على اسمها عن طريق فحص السجلات التي يتم إرجاعها بواسطة **dmesg**.

```
$ dmesg
[...]
[234743.896134] usb 1-1.2: new high-speed USB device number 6 using ehci-pci
[234743.990764] usb 1-1.2: New USB device found, idVendor=08ec, idProduct=0020
[234743.990771] usb 1-1.2: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[234743.990774] usb 1-1.2: Product: Store'n'go
[234743.990777] usb 1-1.2: Manufacturer: Verbatim
[234743.990780] usb 1-1.2: SerialNumber: 0390627052A2F897
[234743.991845] usb-storage 1-1.2:1.0: USB Mass Storage device detected
[234743.992017] scsi host7: usb-storage 1-1.2:1.0
[234744.993818] scsi 7:0:0:0: Direct-Access     VBTM     Store'n'go 6.51 PQ: 0 ANSI: 0 CCS
[234744.994425] sd 7:0:0:0: Attached scsi generic sg1 type 0
[234744.995753] sd 7:0:0:0: [sdb] 3903487 512-byte logical blocks: (2.00 GB/1.86 GiB)
[234744.996663] sd 7:0:0:0: [sdb] Write Protect is off
[234744.996669] sd 7:0:0:0: [sdb] Mode Sense: 45 00 00 08
```

```
[234744.997518] sd 7:0:0:0: [sdb] No Caching mode page found
[234744.997524] sd 7:0:0:0: [sdb] Assuming drive cache: write through
[234745.009375] sdb: sdb1
[234745.015113] sd 7:0:0:0: [sdb] Attached SCSI removable disk
```

الآن بعد أن عرفت أن مسار مفتاح USB هو dev/sdb/، يمكنك المتابعة لنسخ الصورة باستخدام الأمر **dd**:

```
#dd if=kali-linux-light-2016.2-amd64.iso of=/dev/sdb
2070784+0 records in
2070784+0 records out
1060241408 bytes (1.1 GB, 1011 MiB) copied, 334.175 s, 3.2 MB/s
```

لاحظ أنك بحاجة إلى أذونات الجذر لإتمام هذه العملية ويجب عليك أيضًا التأكد من عدم استخدام مفتاح USB. وهذا هو، يجب عليك التأكد من أنه لا يوجد أي جزء منه موصول. يفترض الأمر أيضًا أنه يتم تشغيله أثناء وجوده في المجلد الذي فيه صورة ISO، وإلا فسيتعين توفير المسار الكامل.

للعلم: **if** تعني "ملف الإدخال" و **of** "ملف الإخراج". يقوم الأمر **dd** بقراءة البيانات من ملف الإدخال وإعادة كتابتها مرة أخرى إلى ملف الإخراج. لا يُظهر أي معلومات تَقَدُّم، لذا يجب عليك التحلي بالصبر أثناء قيامه بعمله (ليس من غير المعتاد أن يستغرق الأمر أكثر من نصف ساعة!). انظر إلى مصباح نشاط الكتابة على مفتاح USB إذا كنت ترغب في التحقق من أن الأمر يعمل. يتم عرض الإحصاءات المبينة أعلاه فقط عند اكتمال الأمر.

على **OS X / macOS**، يمكنك أيضًا الضغط على CTRL + T أثناء العملية للحصول على معلومات إحصائية عن النسخة بما في ذلك كمية البيانات التي تم نسخها.

٣.٤.١.٢. إنشاء محرك أقراص USB قابل للإقلاع من OS X/mac OS

يعتمد نظام OS X/macOS على نظام UNIX، لذا فإن عملية إنشاء محرك أقراص Kali Linux USB قابل للإقلاع تشبه إجراء Linux. بمجرد قيامك بتنزيل والتحقق من ملف Kali ISO الذي اخترته، استخدم أمر **dd** لنسخه على مفتاح USB.

لتحديد اسم جهاز مفتاح USB، قم بتشغيل قائمة **diskutil** لسرد الأقراص المتوفرة على نظامك. بعد ذلك، أدخل مفتاح USB وقم بتشغيل أمر قائمة **diskutil** مرة أخرى. يجب أن يكون ثاني نتيجة للقرص الإضافي. يمكنك تحديد اسم الجهاز لمفتاح USB عن طريق مقارنة الإخراج من كلا الأمرين. ابحث عن سطر جديد يحدد قرص USB ولاحظ dev/diskX/ حيث يمثل X معرف القرص.

يجب عليك التأكد من عدم وصل مفتاح USB، والذي يمكن تنفيذه باستخدام أمر **unmount** (بافتراض أن dev/disk6/ هو اسم جهاز مفتاح USB):

```
$ diskutil unmount /dev/disk6
```

الآن انتقل إلى تنفيذ الأمر **dd**. هذه المرة، نضيف معلمة تكميلية **bs-** لحجم الكتلة. يحدد حجم الكتلة التي تتم قراءتها من ملف الإدخال ثم يتم كتابتها إلى ملف الإخراج.

```
# dd if=kali-linux-light-2016.2-amd64.iso of=/dev/disk6 bs=1M
1011+0 records in
1011+0 records out
1060241408 bytes transferred in 327.061 secs (3242328 bytes/sec)
```

هذا هو. مفتاح USB جاهز الآن ويمكنك الإقلاع منه أو استخدامه لتثبيت Kali Linux.

إنشاء محرك أقراص USB قابل للإقلاع من سطر الأوامر

> للإقلاع من محرك أقراص بديل على نظام OS X / macOS، بعد تشغيل الجهاز مباشرة اضغط مع الإستمرار على مفتاح option ثم حدد محرك الأقراص الذي تريد الإقلاع منه.

٢.٢. إقلاع نظام كالي في الوضع المباشر

١.٢.٢. على حاسوب حقيقي

كشرط أساسي، تحتاج إما إلى إعداد مفتاح USB (كما هو مفصل في القسم السابق) أو قرص DVD-ROM تم حرقه كصورة Kali Linux ISO.

BIOS / UEFI مسؤول عن عملية الإقلاع المبكر ويمكن تهيئته من خلال برنامج يسمى "Setup". على وجه الخصوص، يسمح للمستخدمين باختيار جهاز الإقلاع المفضل. في حالتنا، نريد تحديد محرك أقراص DVD-ROM أو محرك أقراص USB، اعتماداً على الجهاز الذي قمت بإنشائه.

يتضمن بدء الإعداد عادةً الضغط على مفتاح معين في وقت قريب جدًا بعد تشغيل الحاسوب. غالبًا ما يكون هذا المفتاح هو Del أو Esc، وأحيانًا F2 أو F10. في معظم الأوقات، يبقى وقت الاختيار لفترة قصيرة على الشاشة عندما يشتغل الحاسوب، قبل تحميل نظام التشغيل.

بمجرد تهيئة BIOS/UEFI بشكل صحيح للإقلاع من جهازك، فإن تشغيل Kali Linux هو مجرد إدخال قرص DVD-ROM أو توصيله في محرك USB وتشغيله على الحاسوب.

تعطيل الإقلاع الآمن

Disable Secure Boot

بينما يمكن تشغيل صور Kali Linux في وضع UEFI، إلا أنها لا تدعم الإقلاع الآمن. يجب عليك تعطيل هذه الميزة في الإعداد.

٢.٢.٢. على جهاز افتراضي

الأجهزة الافتراضية لها فوائد متعددة لمستخدمي Kali Linux. إنها مفيدة بشكل خاص إذا كنت ترغب في تجربة Kali Linux ولكنك غير مستعد للالتزام بتثبيته بشكل دائم على جهازك أو إذا كان لديك حاسوب قوي وتريد تشغيل أنظمة متعددة في وقت واحد. يعد هذا اختيارًا شائعًا للعديد من مختبري الاختراق ومتخصصي الأمان الذين يحتاجون إلى استخدام مجموعة واسعة من الأدوات المتوفرة في Kali Linux ولكن لا يزالون يريدون البقاء في نظام التشغيل الأساسي الخاص بهم. هذا يوفر لهم أيضًا القدرة على أرشفة الجهاز الافتراضي أو حذفه بشكل آمن وأي بيانات عميل قد يحتوي عليها بدلاً من إعادة تثبيت نظام التشغيل بالكامل.

تجعل ميزة اللقطة (Snap) الخاصة ببرامج المحاكاة الافتراضية من السهل تجربة العمليات التي قد تكون خطرة، مثل تحليل البرامج الضارة، مع إتاحة طريقة سهلة عن طريق استعادة اللقطة السابقة.

هناك العديد من أدوات المحاكاة الافتراضية المتاحة لجميع أنظمة التشغيل الرئيسية، بما في ذلك VirtualBox® و VMware Workstation® و Xen و KVM و Hyper-V على سبيل المثال لا الحصر. في النهاية، استخدم البرنامج الذي يناسبك، لكننا سنغطي اثنين الأكثر استخدامًا في مجال سطح المكتب: VirtualBox® و VMware Workstation Pro®، وكلاهما يعمل على Windows 10. إذا لم يكن لديك قيود سياسة الشركة أو التفضيل الشخصي، توصيتنا هي أن تجرب VirtualBox أولاً، لأنها مجانية، وتعمل بشكل جيد، (غالبًا) مفتوحة المصدر، ومتاحة لمعظم أنظمة التشغيل. بالنسبة إلى الفصول التالية، سنفترض أنك قمت بالفعل بتثبيت أداة المحاكاة الافتراضية المناسبة وأنك على علم بطريقة تشغيلها.

٢.٢.٢.١. ملاحظات مهمة

للاستفادة الكاملة من المحاكاة الافتراضية، يجب أن يكون لديك معالج بالميزات الافتراضية المناسبة ويجب ألا يتم تعطيلها بواسطة BIOS / UEFI. تحقق مرة أخرى من خيارات "**تقنية المحاكاة الافتراضية من ®Intel**" و / أو "**ميزة Intel® VT-d**" في شاشة الإعداد.

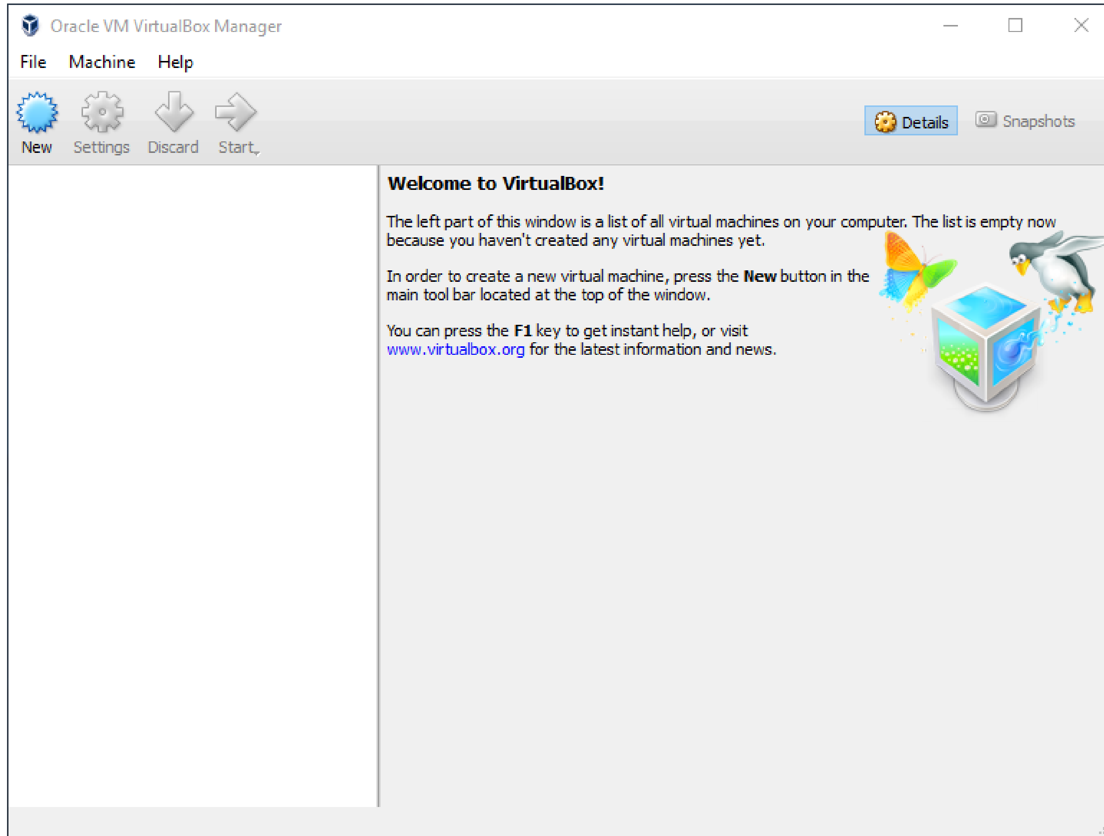
يجب أن يكون لديك أيضًا نظام تشغيل 64 bit، مثل بنية amd64 لتوزيعات Linux المستندة على Debain، وبنية x86_64 لتوزيعات Linux المستندة على RedHat، و 64-bit لنظام Windows.

إذا كنت تفتقر إلى أي من المتطلبات الأساسية، فلن تعمل أداة المحاكاة الافتراضية بشكل صحيح أو ستقتصر على تشغيل أنظمة تشغيل 32 bit فقط.

نظرًا لأن أدوات المحاكاة الافتراضية ترتبط بنظام التشغيل والأجهزة المضيفة بمستوى منخفض، فغالبًا ما يكون هناك عدم توافق بينهما. لا تتوقع أن تعمل هذه الأدوات جيدًا في نفس الوقت. احذر أيضًا من أن الإصدارات الاحترافية من Windows تأتي مع تثبيت Hyper-V وتمكينه، مما قد يتداخل مع الأداة الافتراضية التي تختارها. لإيقاف تشغيله، قم بتنفيذ "تشغيل ميزات Windows أو إيقاف تشغيلها" من إعدادات Windows.

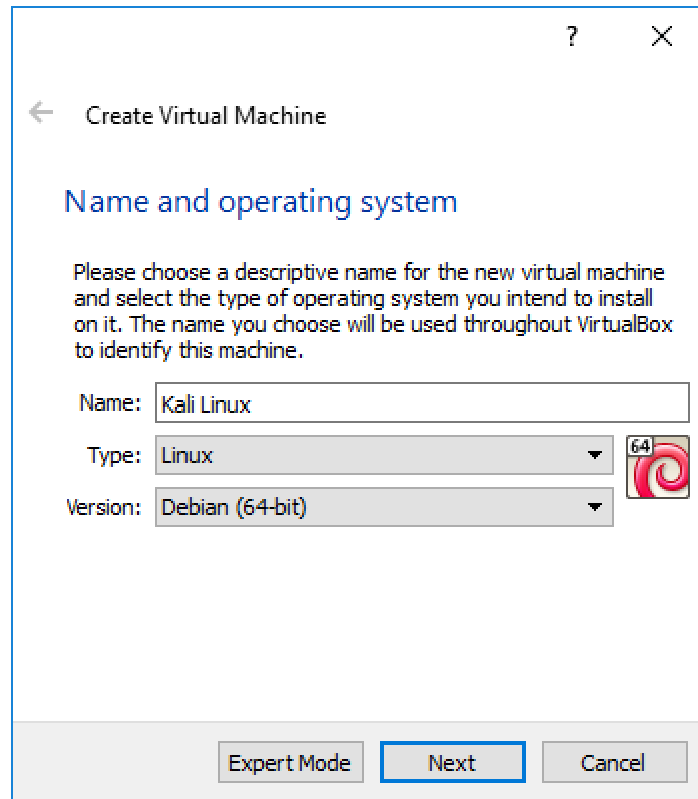
٢.٢.٢.٢. VirtualBox

تبدو الشاشة الرئيسية لـ VirtualBox مثل الشكل ٦.٢، "شاشة بدء VirtualBox".



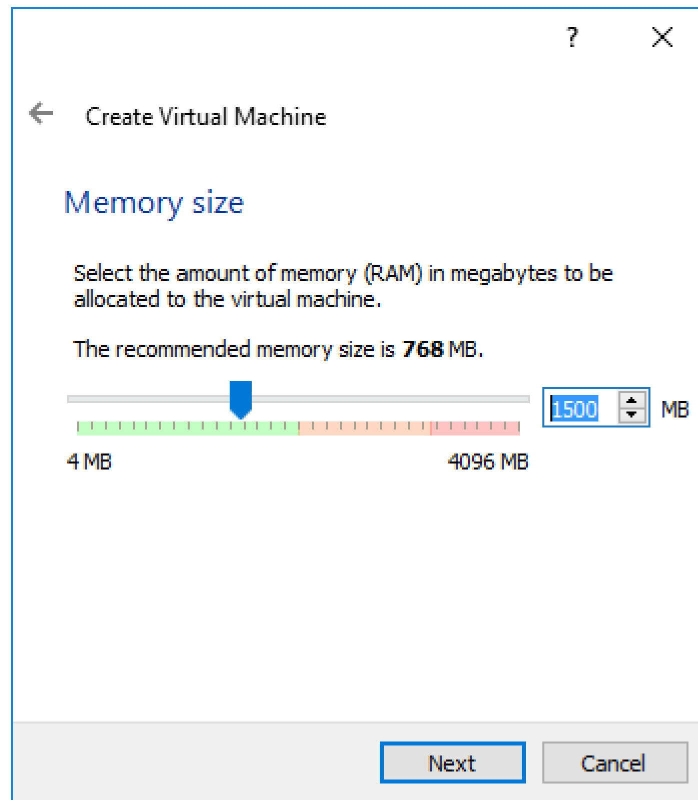
شكل ٦.٢ شاشة بدء VirtualBox

انقر فوق جديد "New" (الشكل ٧.٢ "الاسم ونظام التشغيل") لبدء معالج يرشدك خلال الخطوات المتعددة اللازمة لإدخال جميع معلمات للجهاز الافتراضي الجديد.



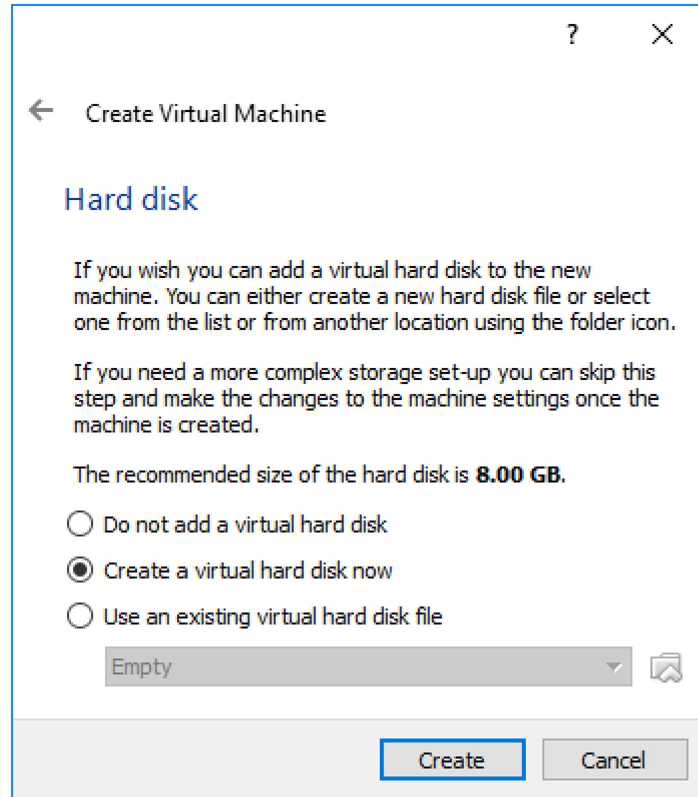
شكل ٧.٢ الاسم ونظام التشغيل

في الخطوة الأولى، الموضحة في الشكل ٧.٢ "الاسم ونظام التشغيل"، يجب تعيين اسم لجهازك الافتراضي الجديد. سوف نستخدم "Kali Linux". يجب أيضًا الإشارة إلى نوع نظام التشغيل الذي سيتم استخدامه. نظراً لأن Kali Linux يستند إلى Debian GNU / Linux، لحدد Linux للنوع و(Debian (32-bit أو Debian (64-bit) للإصدار. على الرغم من أن أي إصدار Linux آخر سيعمل على الأرجح، فإن هذا سيساعد على التمييز بين الأجهزة الافتراضية المختلفة التي ربما تكون قد قمت بتثبيتها.



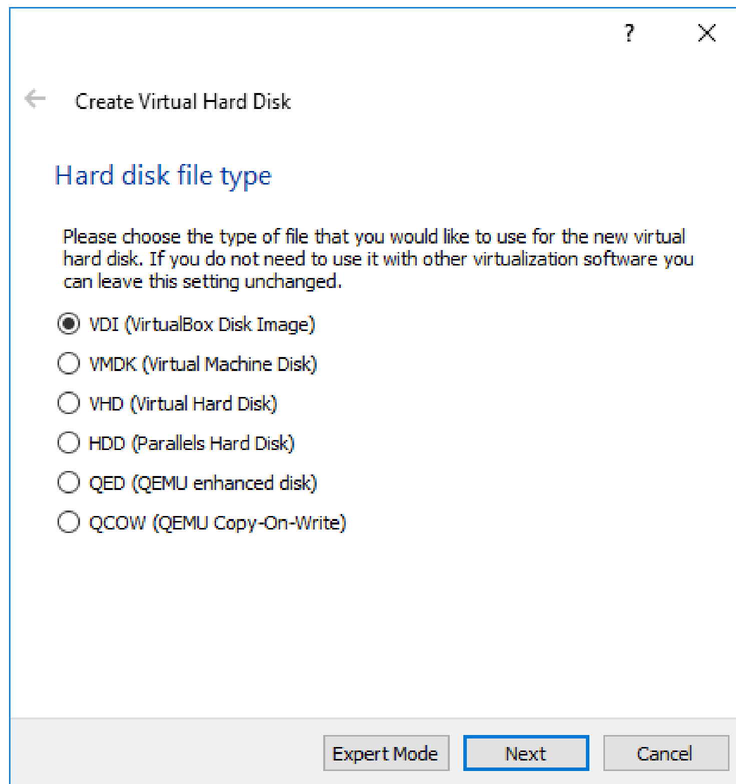
شكل ٨.٢ حجم الذاكرة

في الخطوة الثانية، يجب أن تقرر مقدار الذاكرة المخصصة للجهاز الافتراضي. على الرغم من أن الحجم الموصى به هو 768 MB مقبول لجهاز ديبيان الافتراضي الذي يعمل كخادم، فمن المؤكد أنه لا يكفي تشغيل نظام Kali لسطح المكتب، لا سيما لنظام Kali Linux المباشر لأن النظام المباشر يستخدم الذاكرة لتخزين التغييرات التي تم إجراؤها على نظام الملفات. لقد قمنا بزيادة القيمة إلى 1500 MB (الشكل ٨.٢ "حجم الذاكرة") ونوصي بشدة بتخصيص ما لا يقل عن 2048 MB من ذاكرة الوصول العشوائي (RAM).



شكل ٩.٢. القرص الصلب

في الخطوة الثالثة (الموضحة في الشكل ٩.٢، "القرص الصلب")، تتم مطالبتك باختيار قرص ثابت حقيقي أو افتراضي لجهازك الافتراضي الجديد. على الرغم من أن القرص الصلب ليس مطلوباً لتشغيل Kali Linux كنظام مباشر، إلا أننا سنضيف واحداً حتى نتمكن من عرض إجراء التثبيت لاحقًا في الفصل الرابع، تثبيت Kali Linux.



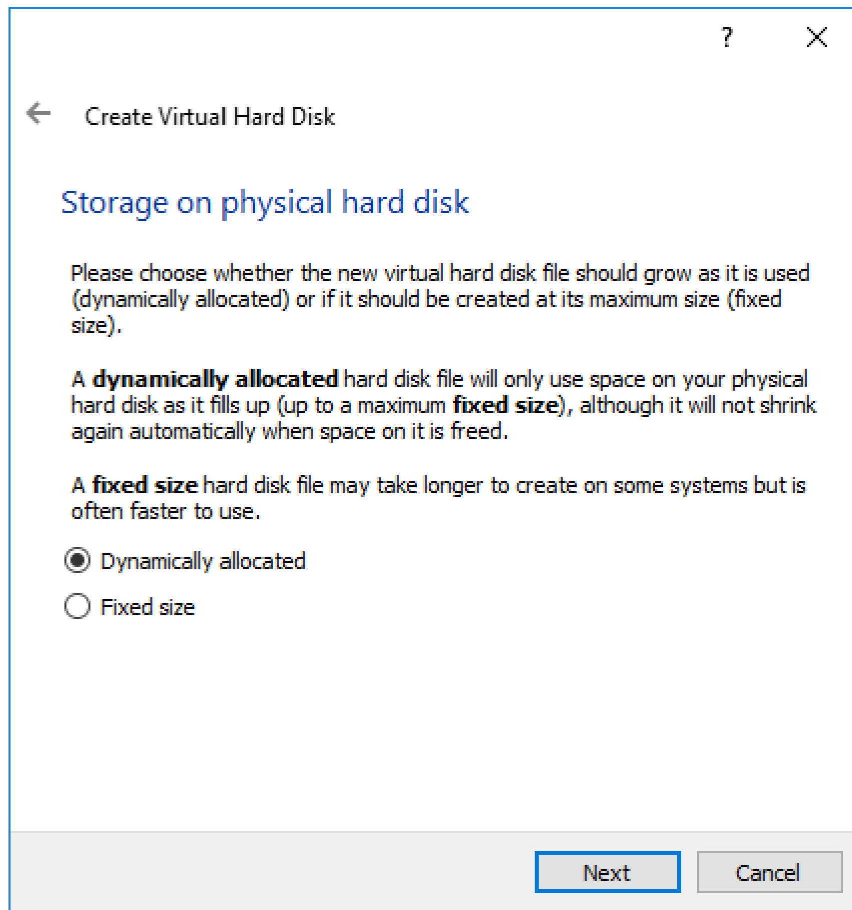
شكل ٢.١٠. نوع ملف القرص الصلب

يتم تخزين محتوى القرص الصلب للجهاز الافتراضي على الجهاز المضيف كملف.

يمكن لـ VirtualBox تخزين محتويات القرص الصلب باستخدام تنسيقات متعددة (كما هو موضح في الشكل ٢.١٠، "نوع ملف القرص الصلب"):

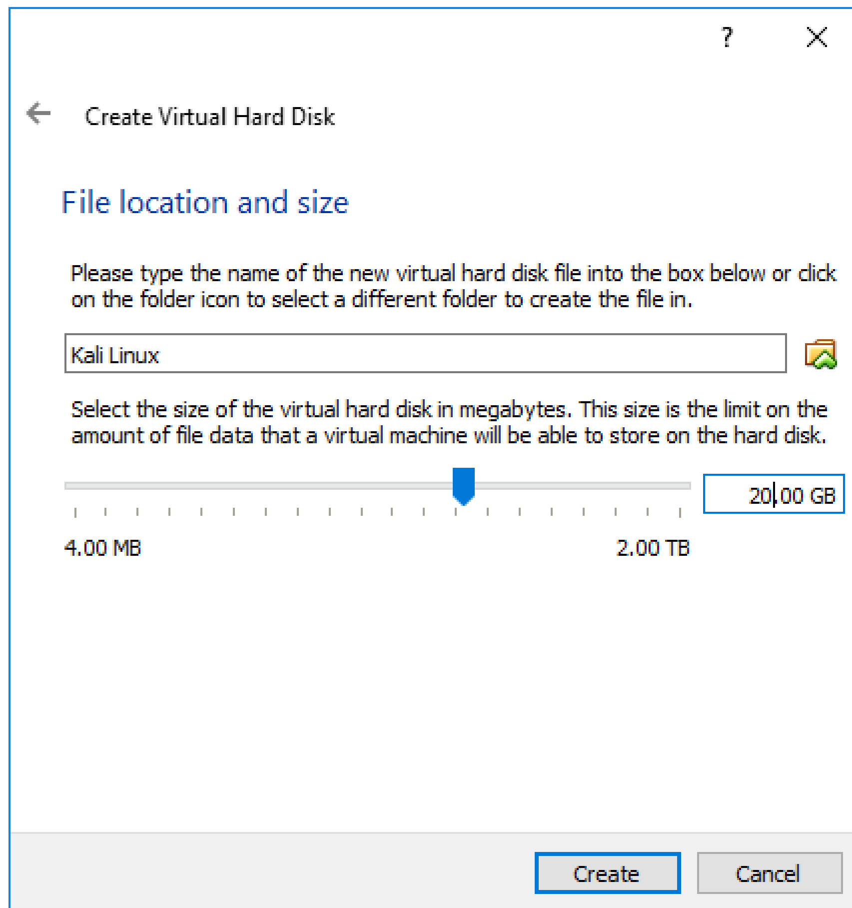
- ❖ يتوافق الإعداد الافتراضي (**VDI**) مع التنسيق الأصلي لـ VirtualBox.
- ❖ **VMDK** هو التنسيق المستخدم بواسطة VMware.
- ❖ **QCOW** هو التنسيق المستخدم بواسطة QEMU.

نحتفظ بالقيمة الافتراضية، لأنه ليس لدينا أي سبب لتغييرها. تعد القدرة على استخدام تنسيقات متعددة مثيرة للاهتمام بشكل أساسي عندما تريد نقل جهاز افتراضي من أداة افتراضية إلى أخرى.



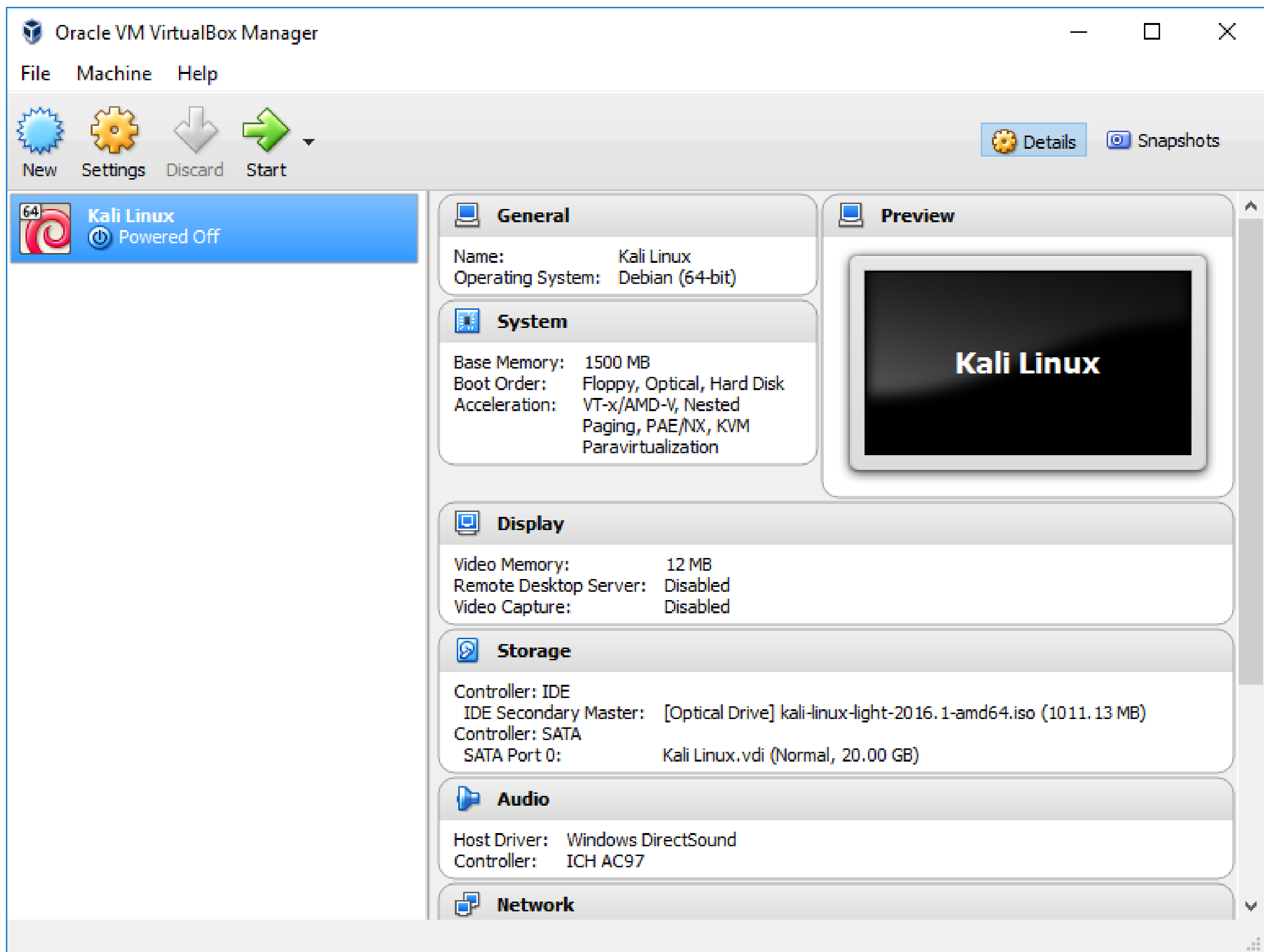
شكل ١١.٢. التخزين على القرص الصلب

يشرح نص التوضيح في الشكل ١١.٢، "التخزين على القرص الصلب" مزايا وعيوب تخصيص القرص الحيوي والثابت. نحن نقبل التحديد الافتراضي (المخصص بشكل حيوي "Dynamically")؛ نظراً لأننا نستخدم حاسوب محمول به أقراص SSD. في حالتنا، لا نريد تضييع المساحة ولن نحتاج إلى أداء إضافي نظراً لأن أجهزتنا سريعة جدًا بالفعل.



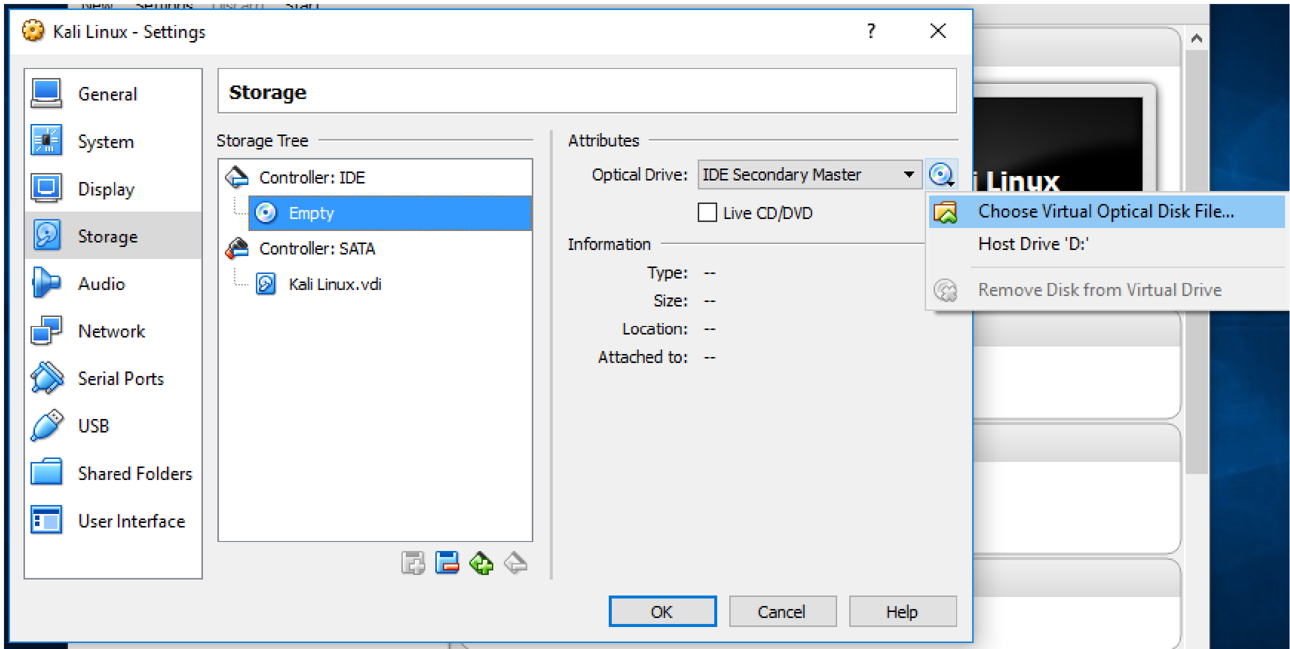
شكل ١٢.٢. موقع الملف وحجمه

لا يكفي حجم القرص الصلب الافتراضي وهو 8 GB الموضح في الشكل ١٢.٢. "موقع الملف وحجمه" للتثبيت القياسي لنظام Kali Linux، وبالتالي نزيد الحجم إلى 20 GB. يمكنك أيضًا تعديل اسم وموقع صورة القرص. يمكن أن يكون ذلك مفيدًا عندما لا يكون لديك مساحة كافية على القرص الصلب، مما يسمح لك بتخزين صورة القرص على محركات أقراص خارجية.



شكل ٢.١٣. يظهر الجهاز الافتراضي الجديد في القائمة

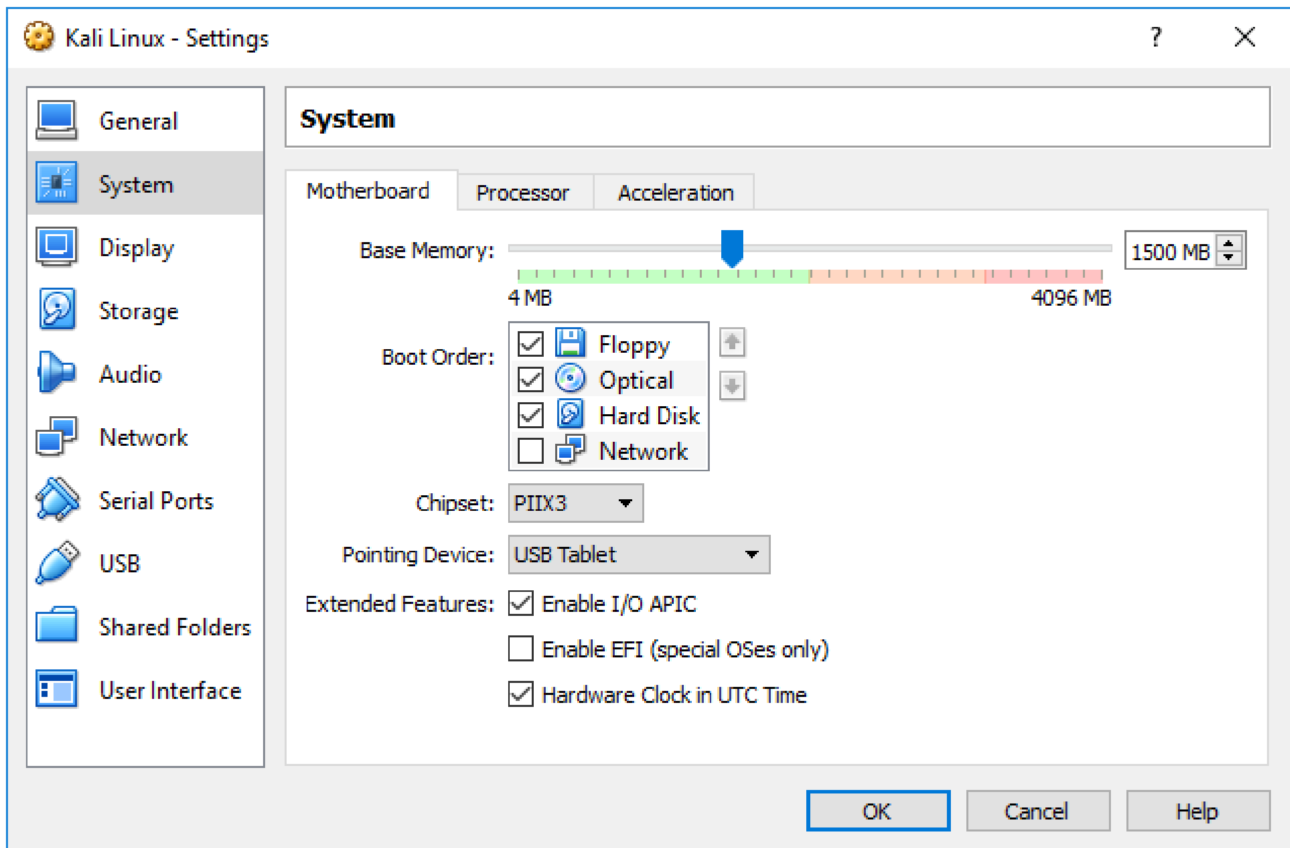
تم إنشاء الجهاز الافتراضي ولكن لا يمكننا تشغيله الان، لأنه لا يوجد نظام تشغيل مثبت. لدينا أيضا بعض الإعدادات للقرص. انقر فوق "الإعدادات (Settings)" على شاشة VM Manager ودعونا نراجع بعض الإعدادات الأكثر فائدة.



شكل ١٤.٢ إعدادات التخزين

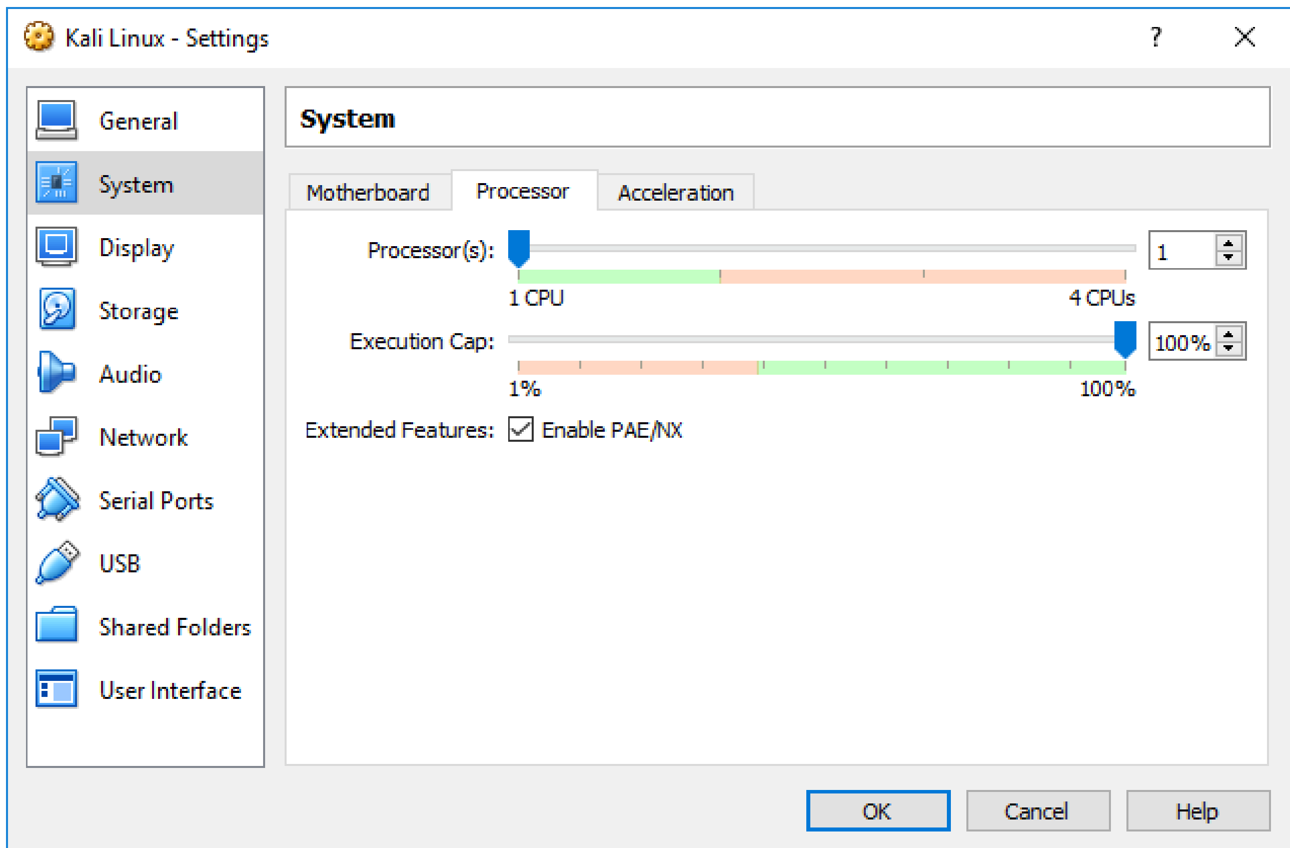
في شاشة التخزين (الشكل ١٤.٢، "إعدادات التخزين")، يجب عليك ربط صورة Kali Linux ISO بقارئ CD / DVD-ROM الافتراضي.

أولاً: حدد محرك الأقراص المضغوطة في قائمة "Storage Tree"، ثم انقر فوق أيقونة الأقراص المضغوطة الصغيرة على اليمين لعرض قائمة متفرعة حيث يمكنك "اختيار ملف القرص الظاهري ... (Choose Virtual Optical Disk File...)".



شكل ١٥.٢. إعدادات النظام: لوحة الأم

في شاشة النظام (الشكل ١٥.٢، "إعدادات النظام: لوحة الأم")، ستجد علامة تبويب "اللوحة الأم". تأكد من أن ترتيب الإقلاع يشير إلى أن النظام سيحاول أولاً الإقلاع من أي جهاز اختياري قبل تجربة القرص الثابت. في هذا التبويب يمكنك تغيير مقدار الذاكرة المخصصة للجهاز الافتراضي أيضا، إذا دعت الحاجة.

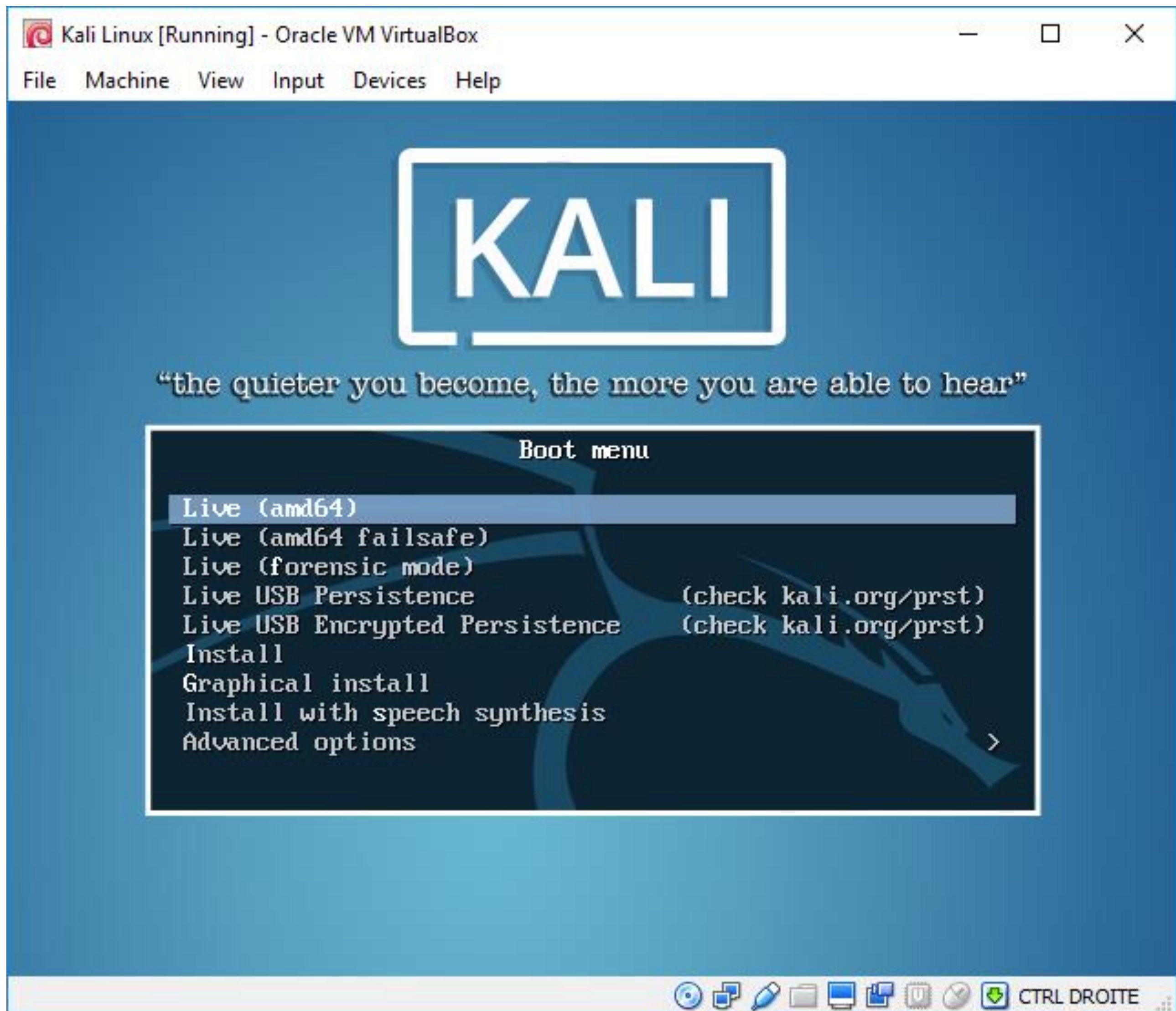


شكل ٢.١٦. إعدادات النظام: المعالج

في نفس الشاشة ولكن ضمن علامة تبويب "المعالج" (الشكل ٢.١٦، "إعدادات النظام: المعالج")، يمكنك ضبط عدد المعالجات المخصصة للجهاز الافتراضي. الأهم من ذلك، إذا كنت تستخدم صورة ذات 32 bit، فلن يتم تمكين PAE / NX أو لن يتم تشغيل صورة Kali نظراً لأن متغير (النواة) kernel الافتراضي الذي تستخدمه Kali لـ i386 (يُسمى بشكل مناسب "pae-686") يتم تجميعه بطريقة تتطلب امتداد عنوان مادي (Physical Address Extension) (PAE) في وحدة المعالجة المركزية.

هناك العديد من المعلمات الأخرى التي يمكن تهيئتها، مثل إعداد الشبكة (تحديد كيفية التعامل مع حركة المرور على بطاقة الشبكة)، ولكن التغييرات المذكورة أعلاه كافية لتتمكن من تشغيل نظام مباشر يعمل بنظام Kali Linux.

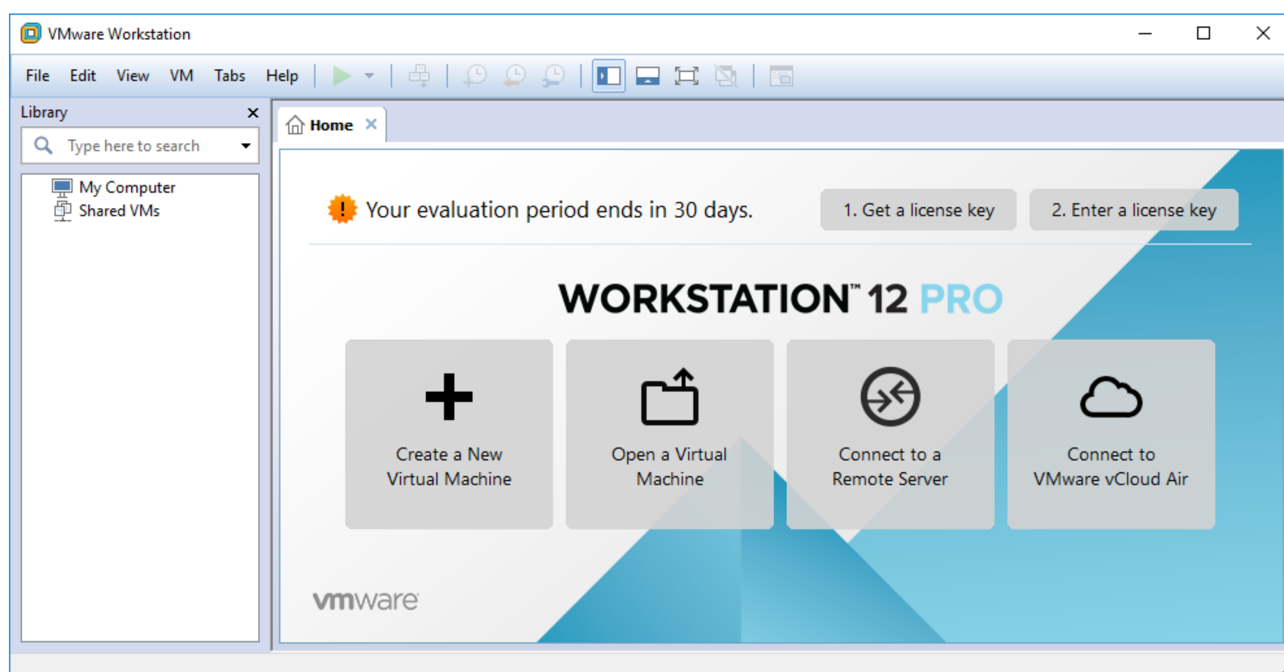
أخيرًا، انقر فوق **Boot** (إقلاع)، يجب على VM الإقلاع بشكل صحيح، كما هو موضح في الشكل ١٧.٢، "شاشة إقلاع كالي لينكس في VirtualBox". إذا لم يكن كذلك، فراجع جميع الإعدادات بعناية وحاول مرة أخرى.



شكل ١٧.٢ شاشة إقلاع كالي لينكس في VirtualBox

٢.٢.٢.٣. VMware

يشبه VirtualBox من حيث الميزات وواجهة المستخدم، لأن كلاهما صُمم خصيصا للاستخدام في أنظمة سطح المكتب، ولكن الإعدادات لجهاز افتراضي جديد مختلفة قليلاً.



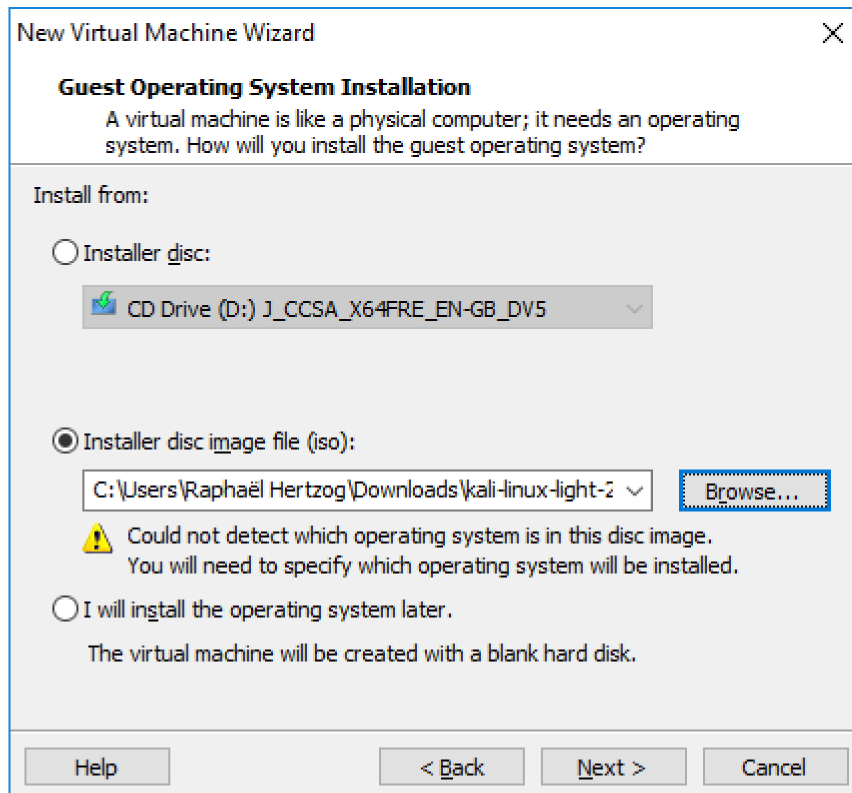
شكل ٢.١٨. شاشة بدء VMware

تعرض شاشة البداية، الموضحة في الشكل ٢.١٨، "شاشة بدء VMware"، زر إنشاء جهاز افتراضي جديد كبير (Create a New Virtual Machine) يقوم بتشغيل معالج لإرشادك خلال إنشاء جهازك الافتراضي.



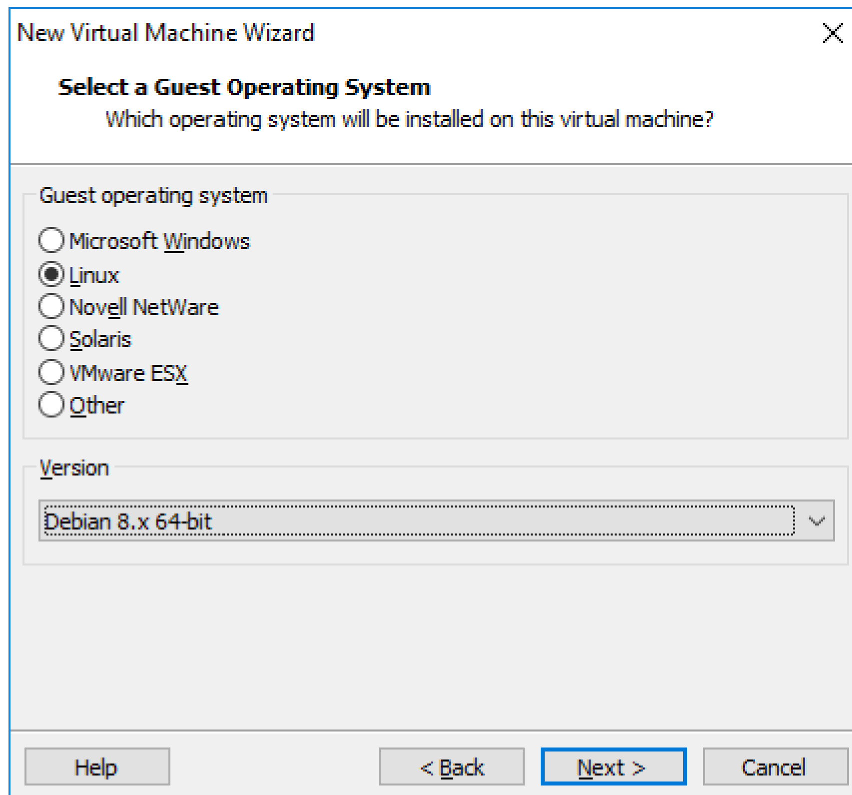
شكل ١٩.٢ معالج الجهاز الافتراضي الجديد

في الخطوة الأولى، يجب أن تقرر ما إذا كنت تريد تقديم الإعدادات المتقدمة أثناء عملية الإعداد أم لا. ليس لدينا أي متطلبات خاصة لذلك اخترنا تثبيتاً نموذجياً (typical installation) كما هو موضح في الشكل ١٩.٢، "معالج الجهاز الافتراضي الجديد".



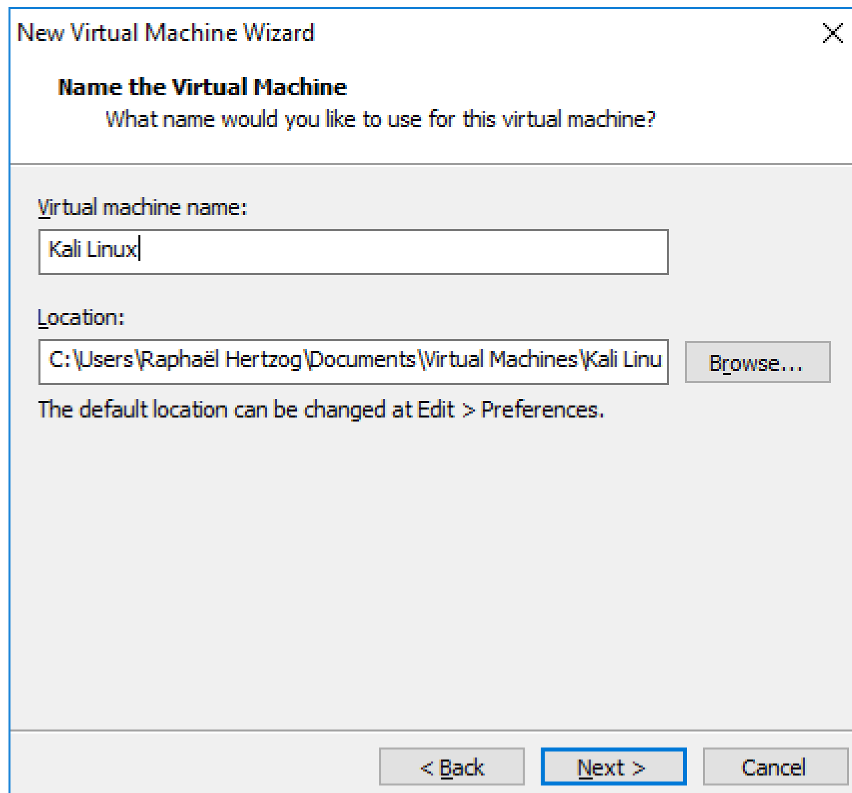
شكل ٢٠.٢ تثبيت نظام التشغيل

يفترض المعالج أنك تريد تثبيت نظام التشغيل على الفور ويطلب منك تحديد صورة ISO التي تحتوي على برنامج التثبيت (الشكل ٢٠.٢، "تثبيت نظام التشغيل"). اختر " Installer disc image file (iso) " وانقر فوق "**Browse**" لتحديد ملف الصورة.



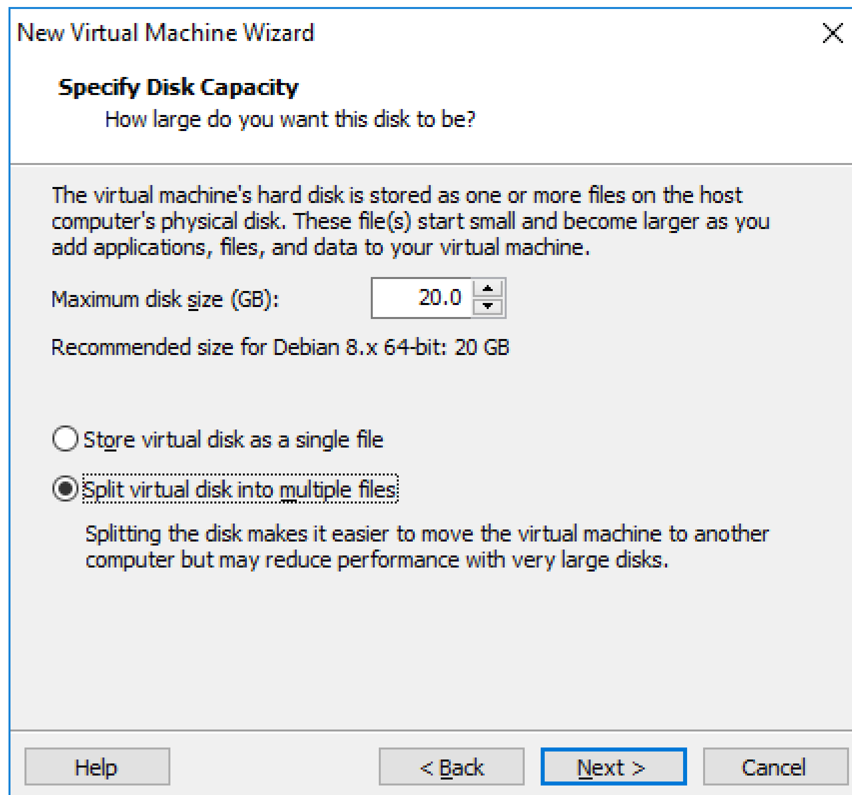
شكل ٢١.٢ اختيار نظام التشغيل

عندما يتعذر اكتشاف نظام التشغيل (OS) من صورة ISO المحددة، يسألك المعالج عن نوع نظام التشغيل الذي تنوي تشغيله. يجب عليك اختيار "Linux" لنظام التشغيل و "Debian 8.x" للإصدار، كما هو مبين في الشكل ٢١.٢، "اختيار نظام التشغيل".



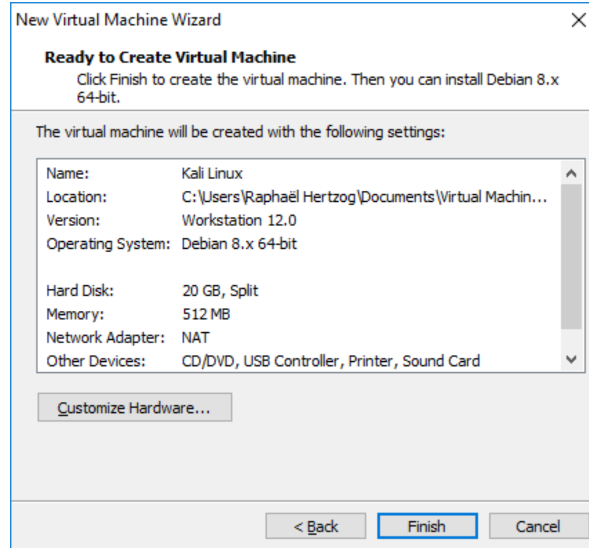
شكل ٢٢.٢ اسم الجهاز الافتراضي

لقد اخترنا Kali Linux كاسم للجهاز الافتراضي الجديد (الشكل ٢٢.٢، "اسم الجهاز الافتراضي"). كما هو الحال مع VirtualBox، لديك أيضًا خيار تخزين ملفات VM في موقع بديل.



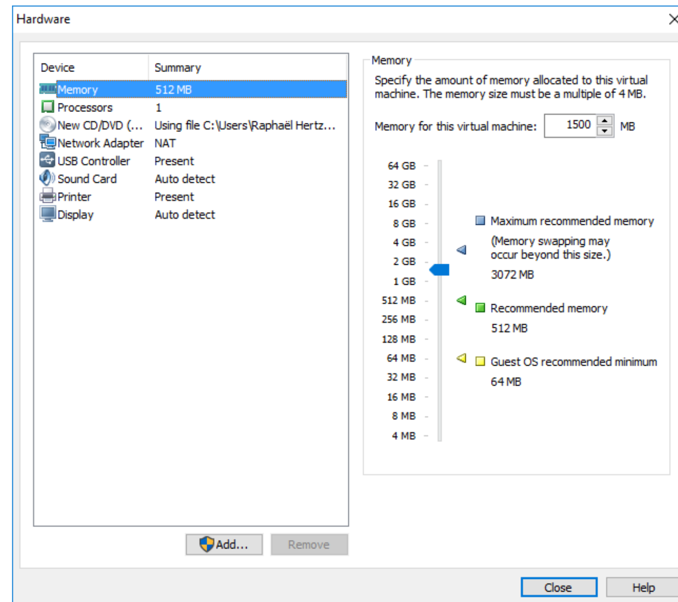
شكل ٢٣.٢ تحديد سعة القرص

عادةً ما يكون حجم القرص الثابت الافتراضي وهو 20 GB (الشكل ٢٣.٢، "تحديد سعة القرص") كافياً ولكن يمكنك ضبطه هنا وفقًا لاحتياجاتك الخاصة. على عكس VirtualBox، والذي يمكنه استخدام ملف واحد بحجم مختلف، فإن VMware لديه القدرة على تخزين محتوى القرص على ملفات متعددة. في كلتا الحالتين، يكون الهدف هو الحفاظ على مساحة قرص نظام التشغيل.



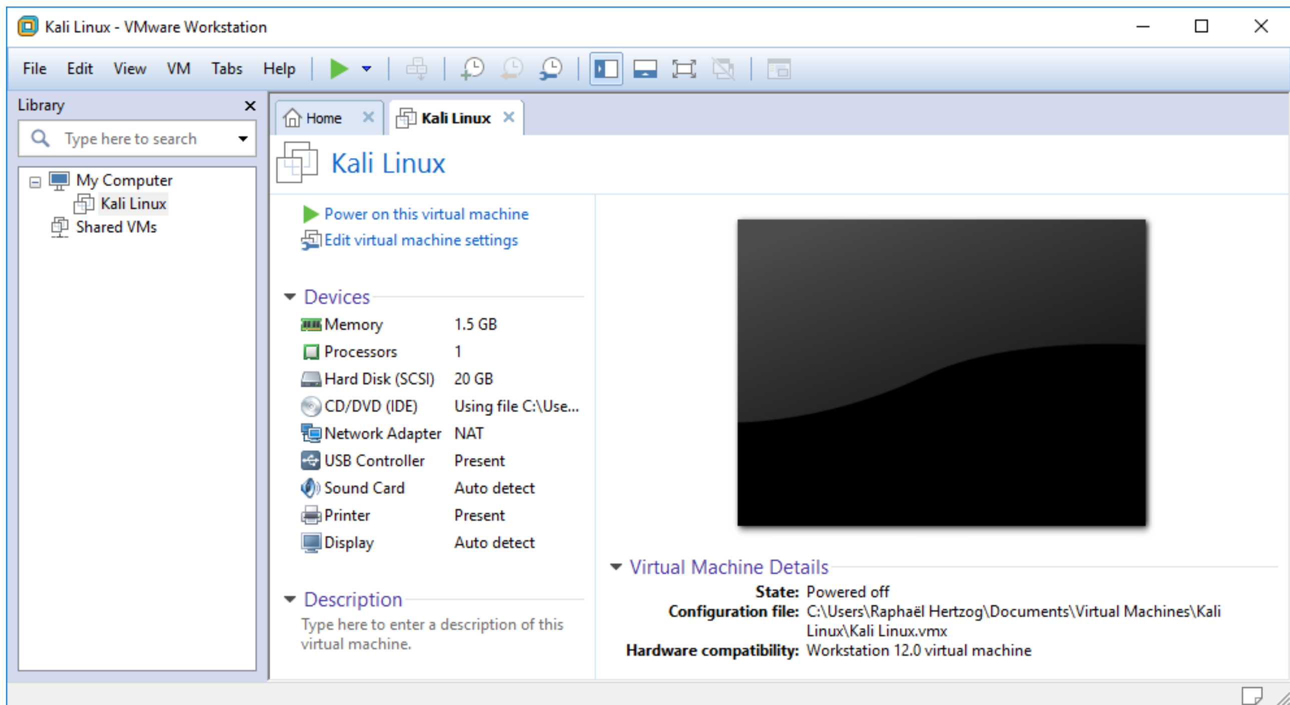
شكل ٢٤.٢ جاهز لإنشاء جهاز افتراضي

تم تكوين VMware Workstation الآن لإنشاء الجهاز الافتراضي الجديد. يعرض ملخصًا للخيارات التي تم إجراؤها حتى تتمكن من التحقق من كل شيء قبل إنشاء الجهاز. ستلاحظ أن المعالج اختار تخصيص MB فقط من ذاكرة الوصول العشوائي للجهاز الافتراضي، وهذا لا يكفي لذلك انقر على ...Customize Hardware (الشكل ٢٤.٢، "جاهز لإنشاء جهاز افتراضي") وقرص إعداد الذاكرة، كما هو مبين في الشكل ٢٥.٢، " نافذة تكوين الهادروير".



شكل ٢٥.٢ نافذة تكوين الهارد وير

بعد نقرة أخيرة على **Finish** (الشكل ٢٤.٢، "جاهز لإنشاء جهاز افتراضي")، تم تكوين الجهاز الافتراضي الآن ويمكن تشغيله بالنقر فوق "Power on this virtual machine" كما هو مبين في الشكل ٢٦.٢، " الجهاز الافتراضي (kali linux) جاهز ".



شكل ٢٦.٢ الجهاز الافتراضي "kali linux" جاهز

٣.٢. الملخص

في هذا الفصل، تعرفنا على مختلف صور Kali Linux ISO وتعلمنا كيفية التحقق منها وتنزيلها، وتعلمنا كيفية إنشاء أقراص USB قابلة للإقلاع من على أنظمة تشغيل مختلفة. ناقشنا أيضًا كيفية تشغيل أقراص USB واستعرضنا كيفية تكوين إعدادات BIOS والإقلاع من وسائط متعددة مختلف، اخترنا وسيط وهو أقراص USB.

نصائح الملخص:

- ❖ www.kali.org هو موقع التنزيل الرسمي الوحيد لـ Kali ISOs. لا تقم بتنزيلها من أي موقع آخر، لأن هذه التنزيلات قد تحتوي على برامج ضارة.
- ❖ تحقق دائمًا من صحة sha256sum للتنزيلات باستخدام الأمر **`sha256sum`** لضمان سلامة تنزيل الصور الخاصة بك. إذا لم يتطابق، فحاول التنزيل مرة أخرى أو استخدم مصدر مختلف.
- ❖ يجب أن تحرق صورة Kali Linux ISO على وسائط قابلة للإقلاع إذا كنت تريد تشغيلها على جهاز حقيقي.
  - ❖ استخدم *Win32 Disk Imager* على Windows.
  - ❖ أو الأداة Disks utility على Linux.
  - ❖ أو الأمر **`dd`** على Mac OS X / macOS.

كن حذرا جدا عند حرق الصورة. قد يؤدي تحديد القرص الخطأ إلى إتلاف البيانات الموجودة على جهازك نهائيًا.

- ❖ قم بتكوين BIOS / UEFI من شاشة الإعدادات وذالك بالضغط على مفتاح Option لنظام OS X / macOS للسماح للجهاز بالاقلاع من محرك USB.

❖ تعد برامج الجهاز الافتراضي مثل *VirhtualBox* و *VMware Workstation Pro* *مفيدة* بشكل خاص إذا كنت ترغب في تجربة Kali Linux ولكنك غير مستعد للالتزام بتثبيته بشكل دائم على جهازك أو إذا كان لديك نظام قوي وتريد تشغيل أنظمة تشغيل متعددة في وقت واحد.

الآن بعد أن تعلمت تثبيت Kali Linux، فقد حان الوقت للتطرق إلى بعض أساسيات Linux المطلوبة لتشغيل Kali الأساسي والمتقدم. إذا كنت من مستخدمي Linux المتوسطين أو المتقدمين، تخطي الفصل التالي.

الإختبار الأول للفصل الثاني: إعداد كالي وتنزيله والتحقق منه وحرقه

قم بتثبيت برنامج جهاز إفتراضي (VM)، مثل (OSX) VMWare Fusion أو VirtualBox، أو غيره.

قم بتنزيل إصدار Kali Linux VM (حبذا لو يكون 64 bit).

قم بإقلاع نظام كالي الافتراضي

من هذه النقطة، يجب أن تكون في VM. تسجيل الدخول إلى VM (toor/root) ونزل صورة kali 64-bit من https://www.kali.org/downloads في Kali VM الخاص بك.

قم بتنزيل واستيراد مفاتيح kali العامة.

استخرج بصمات الإصبع (fingerprint) واحصل على SHA256SUMS وملف التوقيع المقترن مع صورة kali.

تحقق من أن المجموع الإختباري لصورة كالي التي قمت بتنزيلها متطابقة تماما مع المجموع الإختباري الموجود في موقع كالي.

أنشئ جهاز USB قابل للإقلاع بالصورة التي عندك.

الإجابات:

يجب ألا تحتاج للمساعدة في تثبيت برنامج VM.

يجب ألا تحتاج للمساعدة في تنزيل نظام كالي، إذا احتجت للمساعدة في هذا، فهذه الدورة ليست لك.

قم باستخراج ملف Kali VM .7z.

نزل صورة نظام كالي، لاحظ أنه خلال هذا التمرين، قد تختلف أرقام نسختك:

```
wget http://cdimage.kali.org/kali-2017.1/kali-linux-2017.1-amd64.iso
```

نزل واستخرج مفاتيح كالي العامة:

```
wget -q -O - https://www.kali.org/archive-key.asc | gpg --import
```

استخرج بصمات الإصبع واحصل على المجموع الإختباري للصورة.

```
gpg --fingerprint 44C6513A8E4FB3D30875F758ED444FF07D8D0BF6
wget http://cdimage.kali.org/kali-2017.1/SHA256SUMS
wget http://cdimage.kali.org/kali-2017.1/SHA256SUMS.gpg
```

الأن، سوف تحقق من التوقيع، لمعرفة ما إذا كان ملف المجموع الإختباري أصلي:

```
gpg --verify SHA256SUMS.gpg SHA256SUMS
```

يجب أن تشاهد تأكيداً: "توقيع جيد"

لكن انتظر، هناك تحذير قبيح يخيفني!

```
gpg: WARNING: This key is not certified with a trusted signature!
```

* ترجمة: هذا المفتاح غير معتمد بتوقيع موثوق به!*

هذا التحذير طبيعي. يمكنك تجنب ذلك باستخدام خيار "الثقة دائمًا".

```
-trust-model always
```

يقول التحذير فقط أنه لا يوجد طريق بين مجموعة المفاتيح الموثوقة ومفتاح Kali في شبكة الثقة. إذا لم يكن لديك أي مفتاح و/أو إذا لم توقع أبدًا على أي شخص آخر، فلن تتمكن أبدًا من الحصول على مسار ثقة لأي مفتاح آخر.

الآن بعد أن تعرف أن ملف SHA256SUMS أصلي، يمكنك الوثوق بالتجزئة الموجودة في هذا الملف. الآن، احصل على مجموع SHA من ISO الذي قمت بتنزيله:

```
root@kali:~# shasum -a 256 ./kali-linux-2017.1-amd64.iso
49b1c5769b909220060dc4c0e11ae09d97a270a80d259e05773101df62e11e9d  ./kali-linux-2017.1-amd64.iso
```

قارن الهاش الخاصة بك مع الهاش المدرج في ملف المجموع الاختباري (موثوق به الان):

```
root@kali:~# grep kali-linux-2017.1-amd SHA256SUMS
49b1c5769b909220060dc4c0e11ae09d97a270a80d259e05773101df62e11e9d  kali-linux-2017.1-amd64.iso
```

إذا لم يتطابق الهاشان، فقد ارتكبت خطأً (أو حدث لك شيء خاطئ!).

ضع محرك USB الخاص بك، وقم بوصله في VM، وابحث عنه باستخدام **dmesg**، واحرق الصورة القابلة للإقلاع باستخدام شيء مثل هذا. توخ الحذر! هذا مدمر! استخدم مسار القرص الصحيح (dev/sdb/ في حالتنا)!

```
root@kali:~# dmesg
[٤١١٧,١٣٢٨١١ ]usb 1-1: new high-speed USB device number 2 using ehci-pci
[٤١١٧,٢٨٧٣١٩ ]usb 1-1: New USB device found, idVendor=0781, idProduct=5583
[٤١١٧,٢٨٧٣٢١ ]usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[٤١١٧,٢٨٧٣٢٢ ]usb 1-1: Product: Ultra Fit
[٤١١٧,٢٨٧٣٢٢ ]usb 1-1: Manufacturer: SanDisk
[٤١١٧,٢٨٧٣٢٣ ]usb 1-1: SerialNumber: 4C530001231103111240
[٤١١٧,٤٠٧٩٠٢ ]usb-storage 1-1:1.0: USB Mass Storage device detected
[٤١١٧,٤٠٨٨٥٥ ]scsi host3: usb-storage 1-1:1.0
[٤١١٧,٤١٠٣٧٠ ]usbcore: registered new interface driver usb-storage
[٤١١٧,٤٦٥٣٨٦ ]usbcore: registered new interface driver uas
[٤١١٨,٤٢١٣٠٨ ]scsi 3:0:0:0: Direct-Access    SanDisk  Ultra Fit       1.00 PQ: 0 ANSI: 6
[٤١١٨,٤٢٩١٠٧ ]sd 3:0:0:0: Attached scsi generic sg2 type 0
[٤١١٨,٤٣٢١٥١ ]sd 3:0:0:0: [sdb] 242614272 512-byte logical blocks: (124 GB/116 GiB(
[٤١١٨,٤٣٨٧٠٩ ]sd 3:0:0:0: [sdb] Write Protect is off
[٤١١٨,٤٣٨٧١٣ ]sd 3:0:0:0: [sdb] Mode Sense: 43 00 00 00
[٤١١٨,٤٤١٩٦٩ ]sd 3:0:0:0: [sdb] Write cache: disabled, read cache: enabled, doesn't support DPO or FUA
[٤١١٨,٤٦٨٩٠٣ ]sdb: sdb1
[ 4118.492354] sd 3:0:0:0: [sdb] Attached SCSI removable disk
root@kali:~# dd if=kali-linux-2017.1-amd64.iso of=/dev/sdb bs=1M
```

2664+1 records in

2664+1 records out

2794307584 bytes (2.8 GB, 2.6 GiB) copied, 93.8987 s, 29.8 MB/s

غذاء الفكر:

ما هي فوائد الإقلاع المباشرة التي يمكنك التفكير بها؟ وما هي الفوائد السيئة؟

سؤال زن لهذا اليوم:

هل يصيبك غرابة أنه يمكنك ببساطة إدخال ISO إلى مفتاح USB والإقلاع منه؟

الإجابة:

يعد Kaliبالإقلاع المباشر رائعًا عندما تريد:

- ❖ الاحتفاظ بنسخة محمولة من Kali في جيبك.
- ❖ اختبار Kali Linux دون إجراء أي تغييرات على جهاز الحاسوب الخاص بك.
- ❖ بحاجة إلى وضع التحقيق الجنائي.

إجابة سؤال زن: كالي (ودبيان) ISO هي صورة هجينة "**isohybrid**". عندما يتم بناء ISO، تقوم الأداة المساعدة syslinux بتشغيل الأمر ***isohybrid*** على ISO، الذي يضيف جزء مجدول إلى ISO، بينما لا يزال يحتفظ به ملف ISO صالح.

السؤال الثاني، للفصل الثاني -إقلاع Kali

١. قم بتشغيل محرك Kali USB الذي قمت بإنشائه في التمرين السابق، واختر الوضع المباشر.
٢. إنشاء ملف 6GB في root/.
٣. ماذا حدث ولماذا؟
٤. تحقق من أن التغييرات لا تستمر في الوضع المباشر عن طريق إعادة التشغيل.

الإجابة:

١. هناك عدة طرق للقيام بهذا. يمكنك إعادة تشغيل الجهاز المضيف الخاص بك، والإقلاع من USB. يمكنك أيضًا الإقلاع من VirtualBox باستخدام USB (ابحث في قوقل عن "boot usb virtualbox ") أو يمكنك تشغيل USB من برنامج VMWare. راجع مقالة kali.org لمزيد من المعلومات حول إقلاع USB من برنامج VMWare.

٢. لإنشاء ملف بحجم 6 GB:

```
dd if=/dev/zero of=test.img bs=1M count=6144
```

٣. في النهاية، ستتلقى رسالة تفيد بأنه "لا توجد مساحة على الجهاز"، على الرغم من أنك قمت بتكوين محرك أقراص ثابت سعة 20 GB ... ماذا حدث؟ حسنًا، نظرًا لأنك في الوضع المباشر، فأنت تعمل في ذاكرة الوصول العشوائي. لذلك كل ما تفعله في "نظام الملفات" يكتب في نهاية المطاف في ذاكرة عشوائية. بمجرد نفاد ذاكرة الوصول العشوائي (RAM) ... تنفد مساحة القرص.



٤. أعد التشغيل، وتحقق من التغيرات التي أجريتها.

الاختبار الثالث، للفصل الثاني- تعديل مدخلات الإقلاع

١. لقد قمنا بالإقلاع من Kali VM أنشأناه مسبقا ومحرك Kali USB. الآن، سنقوم بتشغيله بطريقة أخرى. إقلاع VM من ISO kali. تأكد من أن الشبكة في وضع NAT.
٢. قم بتحرير خيار الإقلاع المباشر وأضف الخيار "الصامت (quiet)" على سطر النواة للحصول على إقلاع أقل مطوّل لأعلى.
٣. تأكد من أن هذا يحدث فرقًا في لفظ إقلاع.
٤. تحقق من معلمات الإقلاع في الوضع المباشر والتحقيق الجنائي. ما هي الاختلافات؟

الإجابات:

للإقلاع من ISO، قم بتوصيل Kali ISO بمحرك الأقراص المضغوطة الافتراضي قبل التشغيل.

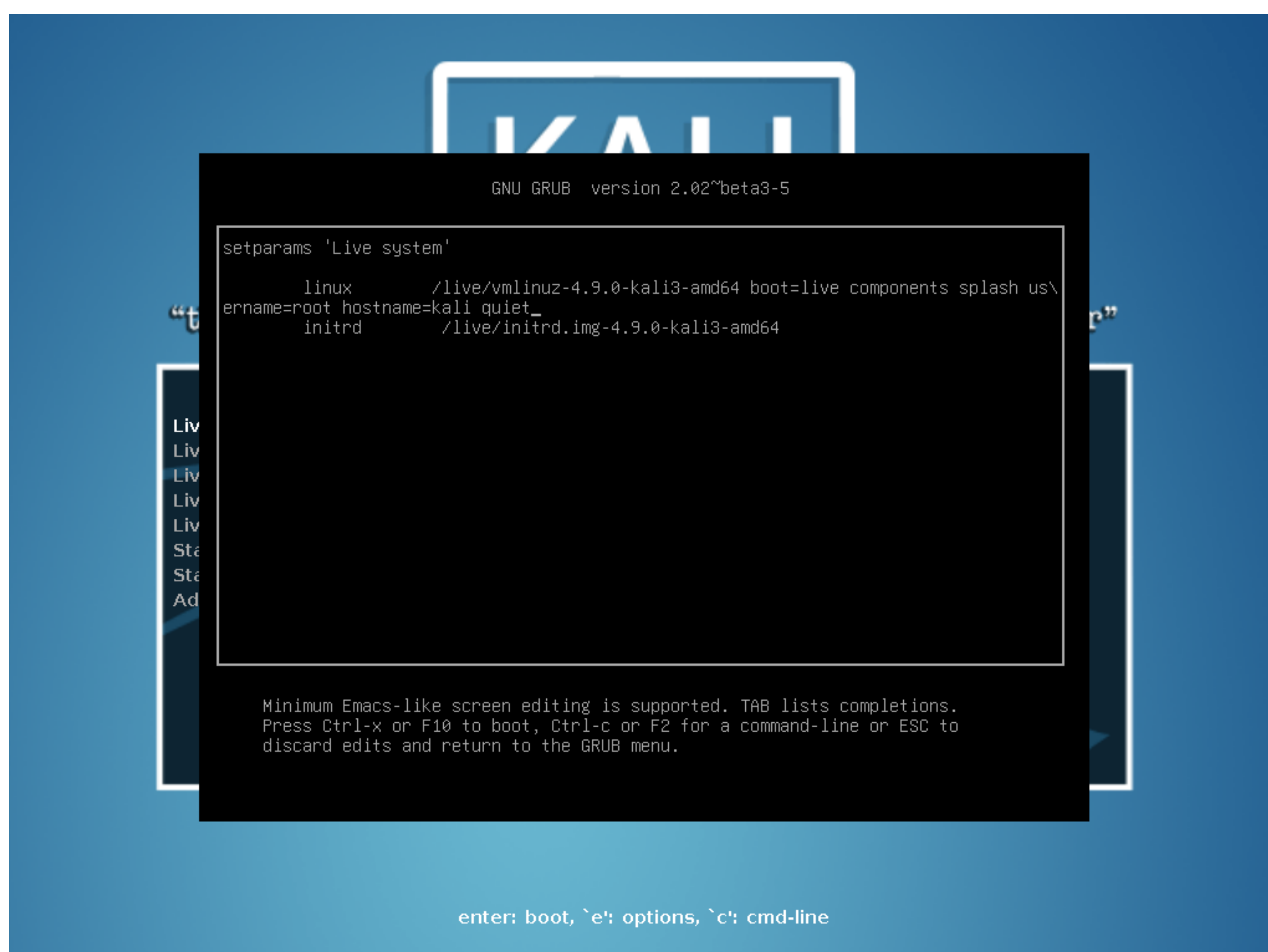
في VMWare، يوجد هذا في:

Virtual Machine > Settings > CD/DVD (IDE)

حدد المربع لتمكين القرص المضغوط، وحدد صورة القرص. لتمكين وضع NAT: في

VMWare> Virtual Machine> Network Adapter

في قائمة الإقلاع، اختر الإقلاع المباشر، واضغط على e وأضف "quiet" إلى سطر linux:



الإقلاع بـ ctrl-x لـ f10.

فعلتها؟

الاختلافات في noswap **ومعلمات الإقلاع** noautomount **والتي توجد في خيار وضع التحقيق الجنائي.**

في حين أن noswap هي معلمة إقلاع ديبيان قياسية، فإن noautomaount هي ميزة محددة من Kali، يتم تنفيذها بواسطة ملف /etc/X11/Xsession.d/52kali_noautomount/، والتي يتم شحنها في حزمة kali-defaults.

اختبار KLCP الثاني

السؤال الأول:

إذا كان لديك سطح مكتب Intel 64-bit، فما صورة كالي التي ستقوم بتشغيلها على جهازك؟ اختر كل ما ينطبق.

- ☐ Kali 32-bit
- ☐ Kali armhf
- ☐ Kali 64-bit
- ☐ Kali armel

السؤال الثاني:

ما الملف الافتراضي الذي يمكنك التحقق منه لتحديد ما إذا كانت وحدة المعالجة المركزية في جهاز Kali Linux الخاص بك هي 32 أو 64 bit؟

- ☐ /proc/cpuflags
- ☐ /proc/cpu
- ☐ /proc/system
- ☐ /proc/cpuinfo

السؤال الثالث:

ما الأمر الذي سيقوم بتنزيل واستيراد مفتاح كالي العام عبر https؟

- ☐ **gpg_import** https://www.kali.org/archive-key.asc
- ☐ **echo** archive-key.asc **| gpg -import**
- ☐ **wget -q -O** – https://www.kali.org/archive-key.asc **| gpg -import**
- ☐ **lynx** http://www.kail.org/archive-key.asc **| gpg_import**

السؤال الرابع:

عند تثبيت Kali Linux على جهاز افتراضي، ما هي طريقة التثبيت التي من المحتمل أن تنتج تثبيتًا نظيفًا؟

- ☐ تنزيله من الموقع الرسمي، التحقق من صورة Kali 32-bit وحرقه على USB.
- ☐ تنزيله من الموقع الرسمي، التحقق من صورة Kali 32-bit ISO وحرقه على USB باستخدام ملف preeseed.cfg الرسمي.
- ☐ تنزيله من الموقع الرسمي، والتحقق من صورة Kali VM.
- ☐ استيراد المثبتة مسبقا، التحقق من صحة واختبار جهاز Kali 32-bit.

الإجابات:

إجابة السؤال الأول:

Kali 32-bit and Kali 64-bit

إجابة السؤال الثاني:

/proc/cpuinfo

إجابة السؤال الثالث:

```
wget -q -O - https://www.kali.org/archive-key.asc
| gpg -import
```

إجابة السؤال الرابع:

تنزيله من الموقع الرسمي، والتحقق من صورة Kali VM.

---((الفصل الثالث))---

٣. أساسيات لِينِكس

قبل أن تتمكن من إتقان Kali Linux، يجب أن تكون مرتاحًا باستخدام نظام Linux. سوف تفيدك الخبرة في نظام Linux، لأنه يمثل نسبة كبيرة من الويب والبريد الإلكتروني وخدمات الإنترنت الأخرى التي تعمل بخوادم Linux.

في هذا الفصل، نسعى جاهدين لتغطية أساسيات Linux، لكننا نفترض أنك تعرف بالفعل أنظمة الحاسوب بشكل عام، بما في ذلك المكونات مثل وحدة المعالجة المركزية (CPU) وذاكرة الوصول العشوائي (RAM) واللوحة الأم والقرص الصلب، بالإضافة إلى وحدات التحكم بالأجهزة والموصلات المرتبطة بها.

١.٣. ما هو لينكس وماذا يفعل؟

غالبًا ما يستخدم مصطلح "Linux" للإشارة إلى نظام التشغيل بالكامل، ولكن في الواقع، Linux هو نواة نظام تشغيل فقط، والذي يتم تشغيله بواسطة أداة محمل الإقلاع، والتي يتم تشغيلها هي نفسها بواسطة BIOS/UEFI. تمثل النواة دورًا مشابهًا لدور موصل في الأوركسترا — فهي تضمن التنسيق بين العتاد والبرامج. يتضمن هذا الدور إدارة الأجهزة والعمليات والمستخدمين والأذونات ونظام الملفات. توفر النواة (kernel) قاعدة مشتركة لجميع البرامج الأخرى الموجودة على النظام وعادةً ما يتم تشغيله في *حلقة الصفر* (*Ring Zero*)، والمعروفة أيضًا باسم مساحة النواة.

مساحة المستخدم

نحن نستخدم مصطلح مساحة المستخدم لجمع كل ما يحدث خارج النواة معًا.

من بين البرامج التي يتم تشغيلها في مساحة المستخدم العديد من الأدوات الأساسية من مشروع GNU، ومعظمها يهدف إلى تشغيلها من سطر الأوامر. يمكنك استخدامها في البرامج النصية لأتمتة العديد من المهام.

لنراجع سريعا المهام المختلفة التي تعالجها نواة لينكس:

٣.١.١. التحكم في العتاد

النواة مكلفة (تعطي الأوامر)، أولاً وقبل كل شيء، بالتحكم في مكونات أجهزة الحاسوب. تكتشفها وتقوم بتكوينها عند تشغيل الحاسوب، أو عند إدخال جهاز أو إزالته (على سبيل المثال، جهاز USB). كما أنها تتيحها للبرامج عالية المستوى، من خلال واجهة برمجة مبسطة، بحيث يمكن للتطبيقات الاستفادة من الأجهزة دون الحاجة إلى معالجة تفاصيل مثل فتحة التمديد التي يتم توصيل لوحة الخيارات بها. توفر واجهة البرمجة أيضًا طبقة تجريدية. يتيح ذلك لبرنامج محادثات الفيديو، على سبيل المثال، استخدام كاميرا ويب بغض النظر عن مصنعها وطرازها. يمكن للبرنامج استخدام واجهة (Video for Linux (V4L وستقوم النواة بترجمة المكالمات الوظيفية للواجهة إلى أوامر العتاد التي تحتاجها كاميرا الويب المحددة المستخدمة.

تقوم النواة بتصدير بيانات حول الأجهزة المكتشفة من خلال أنظمة الملفات الإفتراضية **/proc/** و **/sys/**. غالبًا ما تصل التطبيقات إلى الهاردوير عن طريق الملفات التي يتم إنشاؤها داخل **/dev/**. تمثل ملفات معينة محركات الأقراص (على سبيل المثال، **dev/sda/**)، والأجزاء (**/dev/sda1**)، والفأرة (**/dev/input/mouse0**)، ولوحات المفاتيح (**/dev/input/event0**)، وكرت الصوت (**/dev/snd/***)، المنافذ التسلسلية (**/dev/ttyS***)، والمكونات الأخرى.

هناك نوعان من ملفات الإجهزة: *الكتلة والحرف* (*block* and *character*).

خصائص الكتلة: لديها حجم محدود، ويمكنك الوصول للبايتات في أي موضع في الكتلة.

خصائص الحرف: يمكنك قراءة الأحرف وكتابتها، لكن لا يمكنك البحث عن وظيفة معينة وتغيير وحدات البايت التعسفية.

لمعرفة نوع ملف جهاز معين، انظر للحرف الأول من إخراج أمر:

```
ls -l
```

b: لأجهزة الكتلة، و **c**: لأجهزة الأحرف:

```
$ ls -l /dev/sda /dev/ttyS0
brw-rw---- 1 root disk    8,  0 Mar 21 08:44 /dev/sda
crw-rw---- 1 root dialout 4, 64 Mar 30 08:59 /dev/ttyS0
```

كما ترى، تستخدم محركات الأقراص والأجزاء أجهزة الكتلة، بينما تستخدم الفأرة ولوحة المفاتيح والمنافذ التسلسلية أجهزة الأحرف. في كلتا الحالتين، تتضمن واجهة البرمجة أوامر خاصة بالجهاز والتي يمكن استدعاءها من خلال نظام يسمى *ioctl*.

٢.١.٣ توحيد أنظمة الملفات

أنظمة الملفات هي جانب بارز في النواة. تقوم الأنظمة المشابهة لـ Unix بدمج جميع مخازن الملفات في تسلسل هرمي واحد، مما يتيح للمستخدمين والتطبيقات الوصول إلى البيانات من خلال معرفة موقعها داخل هذا التسلسل الهرمي.

تسمى نقطة الانطلاق لهذه الشجرة الهرمية الجذر(root)، ويمثلها الحرف "/". يمكن أن يحتوي هذا المجلد على مجلدات فرعية. على سبيل المثال، يسمى المجلد الفرعي **الرئيسي** بـ **/home/**. يمكن لهذا المجلد الفرعي أن يحتوي على مجلدات فرعية أخرى، وما إلى ذلك. يمكن أن يحتوي كل مجلد أيضًا على ملفات، حيث سيتم تخزين البيانات. وبالتالي، يشير **/home/buxy/Desktop/hello.txt** إلى ملف يسمى **hello.txt** المخزّن في المجلد الفرعي Desktop والذي هو داخل المجلد الفرعي buxy للمجلد الرئيسي، الموجود في الجذر. تترجم النواة بين نظام التسمية هذا وموقع التخزين على القرص.

بخلاف الأنظمة الأخرى، يمتلك Linux تسلسل هرمي واحد فقط، ويمكنه دمج البيانات من عدة أقراص. يصبح أحد هذه الأقراص هو الجذر، ويتم *وصل* الأقراص الأخرى بالمجلدات في التسلسل الهرمي. (يُطلق على هذا الأمر في Linux **`mount`**) هذه الأقراص الأخرى متوفرة بعد ذلك ضمن نقاط الوصل (mount point). يتيح ذلك تخزين المجلدات الرئيسية للمستخدمين (يتم تخزينها تقليديًا داخل /home/) على قرص ثابت مجزء، والذي سيحتوي على مجلد **buxy** (إلى جانب المجلدات الرئيسية للمستخدمين الآخرين). بمجرد وصل القرص على **/home/**، تصبح هذه المجلدات قابلة للوصول في مواقعها المعتادة، وتستمر المسارات مثل **/home/buxy/Desktop/hello.txt** في العمل.

هناك العديد من تنسيقات نظام الملفات، والتي تقابل العديد من الطرق لتخزين البيانات فعلياً على الأقراص. الأكثر شهرة على نطاق واسع هي *ext2* و *ext3* و *ext4*، ولكن يوجد غيرها. على سبيل المثال، *VFAT* هو نظام الملفات الذي تم استخدامه تاريخيا من قبل أنظمة التشغيل DOS وWindows. يتيح دعم Linux لنظام VFAT إمكانية الوصول إلى الأقراص الصلبة تحت Kali وكذلك في Windows. على أي حال، يجب عليك إعداد نظام ملفات على القرص قبل أن تتمكن من وصله وتُعرف هذه العملية باسم التنسيق (*formatting*). باستخدام أوامر مثل **mkfs.ext3** (حيث **mkfs** اختصار لـ **M**a**K**e **F**ile**S**ystem) تتعامل مع التنسيق. تتطلب هذه الأوامر، كمعلمة، ملف جهاز يمثل الجزء المراد تنسيقه (على سبيل المثال، **/dev/sda1**، الجزء الأول على محرك الأقراص الأول). هذه العملية مدمرة ويجب تشغيلها مرة واحدة فقط، إلا إذا كنت تريد مسح نظام الملفات والبدء من جديد.

هناك أيضًا أنظمة ملفات الشبكة مثل (network filesystems) NFS، التي لا تخزن البيانات على قرص محلي. ولكن بدلا من ذلك، تنقل البيانات عبر الشبكة إلى خادم يقوم بتخزينها واستردادها عند الطلب. بفضل تجريد نظام الملفات، لا داعي للقلق بشأن كيفية الوصول لهذا القرص، حيث تظل الملفات قابلة للوصول بطريقتها الهرمية المعتادة.

٣.١.٣. إدارة العمليات

العملية عبارة عن مثيل قيد التشغيل لبرنامج، والذي يتطلب ذاكرة لتخزين كل من البرنامج نفسه وبيانات التشغيل الخاصة به. النواة هي المسؤولة عن إنشاء وتتبع العمليات. عند تشغيل البرنامج، تقوم النواة أولاً بتخصيص بعض الذاكرة جانبًا، وتقوم بتحميل الكود القابل للتنفيذ من نظام الملفات فيه، ثم يبدأ تشغيل التعليمات البرمجية. يحتفظ بمعلومات حول هذه العملية، وأبرزها هو رقم التعريف المعروف باسم معرف العملية (*process identifier*) (PID).

مثل معظم أنظمة التشغيل الحديثة، فإن تلك التي لها نواة تشبه يونكس، بما في ذلك لينكس، قادرة على تعدد المهام. بمعنى آخر، فهي تسمح للنظام بتشغيل العديد من العمليات في نفس الوقت. هناك بالفعل عملية واحدة قيد التشغيل في أي وقت واحد، لكن النواة تقسم وقت وحدة المعالجة المركزية إلى شرائح صغيرة وتقوم بتشغيل كل عملية بدورها. نظرًا لأن هذه الشرائح الزمنية قصيرة جدًا (في نطاق المللي ثانية)، فإنها تخلق مظهر العمليات التي تعمل بشكل متوازٍ، على الرغم من أنها نشطة فقط خلال الفاصل الزمني الخاص بها وتتوقف عن العمل بقية الوقت. تتمثل مهمة النواة في ضبط آليات الجدولة للحفاظ على هذا المظهر، مع زيادة أداء النظام إلى أقصى حد. إذا كانت شرائح الوقت أطول من اللازم، فقد لا يظهر التطبيق سريع الاستجابة حسب الرغبة. قصير جدًا، ويفقد النظام الوقت عن طريق تبديل المهام كثيرًا جدًا. يمكن تحسين هذه القرارات بأولويات العملية، حيث سيتم تشغيل العمليات ذات الأولوية العليا لفترات أطول وبشرائح زمنية أكثر تكرارًا من العمليات ذات الأولوية المنخفضة.

المعالجات المتعددة (والمتغيرات)

لا يتم تطبيق القيد الموضح أعلاه، وهو عملية واحدة فقط يتم تشغيلها في كل مرة، دائمًا: القيد الفعلي هو أنه لا يمكن أن يكون هناك سوى عملية واحدة قيد التشغيل لكل نواة معالج. تسمح الأنظمة متعددة المعالجات، أو متعددة النواة، أو ذات العمليات المتعددة، بتشغيل عدة عمليات بشكل متوازٍ. ومع ذلك، يتم استخدام نظام تقطيع الوقت نفسه لمعالجة الحالات التي توجد فيها عمليات أكثر نشاطًا من مراكز المعالج المتوفرة. هذا ليس بالأمر غير المعتاد: النظام الأساسي، حتى لو كان خاملاً في الغالب، يحتوي دائمًا على عشرات العمليات الجارية.

تسمح النواة بتشغيل عدة مثيلات مستقلة لنفس البرنامج، لكن يُسمح لكل منها بالوصول فقط إلى شرائح الوقت والذاكرة الخاصة به. وبالتالي تبقى بياناتهم مستقلة.

٤.١.٣. إدارة الحقوق

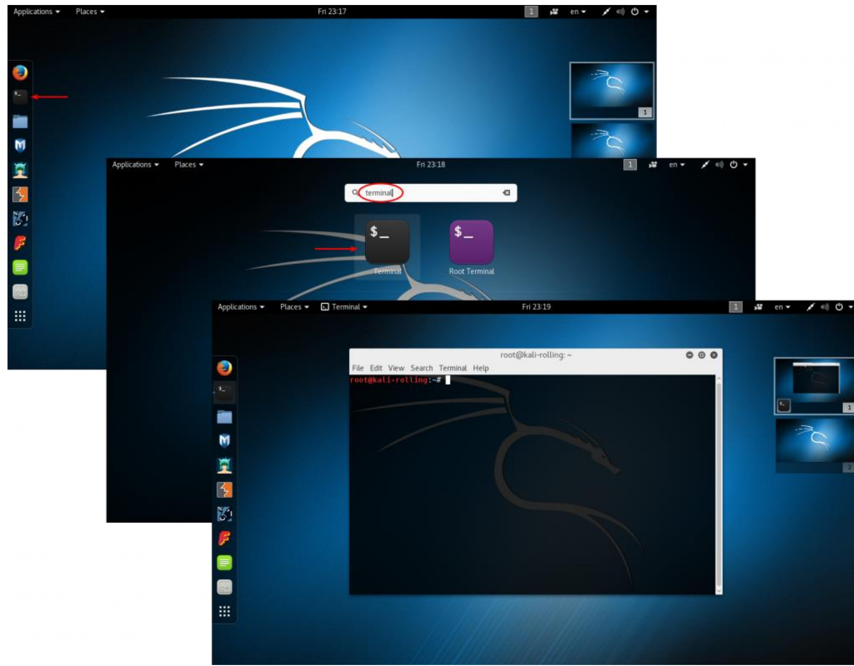
تدعم الأنظمة الشبيهة بيونكس العديد من المستخدمين والمجموعات وتسمح بالتحكم في الأذونات. في معظم الأحيان، يتم تحديد عملية من قبل المستخدم الذي بدأها. لا يُسمح بهذه العملية إلا باتخاذ الإجراءات المسموح بها لمالكها. على سبيل المثال، يتطلب فتح ملف من النواة التحقق من هوية العملية مقابل أذونات الوصول (لمزيد من التفاصيل حول هذا المثال بالذات، انظر باب ٤.٤.٣، "إدارة الحقوق").

٢.٣. سطر الأوامر

نعني بكلمة سطر الأوامر واجهة تعتمد على النصوص، تتيح لك إدخال الأوامر وتنفيدها وعرض النتائج. يمكنك تشغيل الـ(terminal) (شاشة نصية داخل سطح المكتب الرسومي، أو وحدة التحكم في النص نفسها خارج أي واجهة رسومية) الذي يحتوي على مترجم أوامر (shell).

١.٢.٣. كيفية الوصول لسطر الأوامر

عندما يعمل النظام بشكل صحيح، فإن أسهل طريقة للوصول لسطر الأوامر هي تشغيل الـ (terminal) في سطح المكتب.



شكل ١.٣ "بدء تشغيل Gnome terminal"

على سبيل المثال، على نظام kali linux الافتراضي، يمكن تشغيل Gnome Terminal من قائمة التطبيقات المفضلة، يمكنك أيضا كتابة كلمة "**terminal**" أثناء وجودك في شاشة الأنشطة (تلك التي يتم تنشيطها عند تحريك الماوس إلى الزاوية العلوية اليسرى) والنقر على أيقونة التطبيق الصحيح التي تظهر (الشكل ١.٣ "بدء تشغيل Gnome terminal").

في حالة تعطل الواجهة الرسومية الخاصة بك، لا يزال بإمكانك الحصول على واجهة سطر الأوامر بواسطة وحدات التحكم الافتراضية (يمكن الوصول إلى ستة منها من خلال مجموعات المفاتيح الستة CTRL + ALT + F1 إلى - CTRL + ALT + F6 مفتاح CTRL يمكن حذفه إذا كنت بالفعل في شاشة سطر الأوامر، خارج واجهة Xorg أو Wayland الرسومية). يمكنك الحصول على شاشة تسجيل دخول أساسية حيث تدخل معلومات تسجيل الدخول وكلمة المرور الخاصة بك قبل منحك حق الوصول لسطر الأوامر باستخدام الصدفة (shell):

```
Kali GNU/Linux Rolling kali-rolling tty3
kali-rolling login: root
Password:
Last login: Fir Mar 25 12:30:05 EDT 2016 from 192.168.122.1 on pts/2
Linux kali-rolling 4.4.0-kali1-amd4 #1 SMP Debian 4.4.6-1kali1 (2016-03-18) x86_64
The programs included with the Kali GNU/Linux system are free software؛
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali-rolling#~:
```

يُطلق على البرنامج الذي يتعامل مع المدخلات وتنفيذ الأوامر الخاصة بك اسم shell (أو مترجم سطر أوامر).

shell الافتراضي لـ Kali Linux هو Bash (وهو اختصار لـ *Bourne Again Shell*). تشير الـ "**$**" أو "**#**" إلى أن الصدفة تنتظر المدخلات الخاصة بك. يشير أيضًا إلى ما إذا كان Bash يتعرف عليك كمستخدم عادي (**$**) أو كمستخدم فائق (**#**).

٢.٢.٣. أساسيات سطر الأوامر: تصفح شجرة المجلدات وإدارة الملفات

هذا الفصل يعطي فقط نظرة عامة مختصرة على بعض الأوامر، والتي تحتوي جميعها على العديد من الخيارات غير مذكورة هنا، لذا يرجى الرجوع إلى الوثائق الوفيرة المتوفرة في صفحاتها اليدوية. في اختبارات الاختراق، ستحصل غالبًا على وصول shell إلى نظام بعد استغلال ناجح، بدلاً من واجهة مستخدم رسومية. الكفاءة في سطر الأوامر أمر ضروري لنجاحك كمحترف أمني.

|| أقترح عليك قراءة الكتاب المترجم "سطر أوامر لينكس" ||

بمجرد فتح الجلسة:

يعرض الأمر **pwd** (الذي هو اختصار لـ print working directory) موقعك الحالي في نظام الملفات.

يتم تغيير المجلد الحالي باستخدام الأمر:

cd *(اسم أو مسار المجلد)*

cd اختصار لـ(*Change Directory*) عندما لا تحدد المجلد الهدف، يتم نقلك إلى المجلد الرئيسي. عند كتابة أمر **- cd**، ستعود إلى مجلد العمل السابق (المجلد المستخدم قبل اجراء أمر **cd**). يعرف المجلد الأب دائما بـ **..** (نقطتان)، في حين يُعرف المجلد الحالي أيضًا باسم **.** (نقطة واحدة). يسمح الأمر **ls** بسرد محتويات المجلد. إذا لم تكتب معلمات، فسوف تعمل على المجلد الحالي.

```
$pwd
    /home/buxy
$cd Desktop
$pwd
    /home/buxy/Desktop
$cd .
$pwd
    /home/buxy/Desktop
$cd ..
$pwd
/home/buxy
$ls
Desktop     Downloads   Pictures   Templates
Documents   Music       Public     Videos
```

يمكنك إنشاء مجلد جديد باستخدام أمر:

mkdir *(اسم المجلد)*

وإزالة مجلد موجود (فارغ) باستخدام أمر:

rmdir *(اسم المجلد)*

يتيح الأمر **mv** نقل وإعادة تسمية الملفات والمجلدات.

يتم إزالة ملف باستخدام الأمر:

rm *(اسم الملف)*

ويتم نسخ ملف باستخدام الأمر:

cp *(اسم الملف الأصل)* *(اسم الملف الهدف)*

```
$mkdir test
$ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    test
$mv test new
$ls
Desktop    Downloads  new       Public     Videos
Documents  Music      Pictures  Templates
$rmdir new
$ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public
```

تنفّذ الصدفة كل أمر عن طريق تشغيل البرنامج الأول بالاسم المحدد الذي يعثر عليه في المجلد المدرج في بيئة المسار المتغير **PATH**. في معظم الأحيان، تكون هذه البرامج في **bin/** أو **sbin/** أو **usr/bin/** أو **usr/sbin/**. على سبيل المثال، يوجد الأمر **ls** في **bin/ls/**؛ الأمر **which** يبين موقع الملف القابل للتنفيذ. في بعض الأحيان، يتم التعامل مع الأمر مباشرةً بواسطة الصدفة، في هذه الحالة، يطلق عليه أوامر الصدفة (**cd** و **pwd** من بينهن أيضا)؛ يتيح لك الأمر **type** الاستعلام عن نوع كل أمر.

```
$echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
/sbin:/bin
$which ls
/bin/ls
$type rm
rm is /bin/rm
$type cd
cd is a shell builtin
```

لاحظ استخدام الأمر **echo**، والذي يعرض ببساطة النصوص على الـ(terminal). في هذه الحالة، يتم استخدامه لطباعة محتويات متغير بيئة، لأن shell يستبدل المتغيرات تلقائيًا بقيمها قبل تنفيذ سطر الأوامر.

متغيرات البيئة

تسمح متغيرات البيئة بتخزين الإعدادات العامة للصدفة أو البرامج الأخرى المختلفة. فهي سياقية ولكن قابلة للتوريث. على سبيل المثال، تحتوي كل عملية على مجموعة متغيرات البيئة الخاصة بها (فهي سياقية). يمكن أن تقوم الصدفات، مثل صدفة تسجيل الدخول، بإعلان المتغيرات، والتي سيتم نقلها إلى البرامج الأخرى التي تنفذها (وهي قابلة للتوريث).

يمكن تعريف هذه المتغيرات على مستوى النظام في etc/profile/ أو لكل مستخدم في ملف التعريف profile./ ~ ولكن يتم وضع المتغيرات غير الخاصة بمترجمي سطر الأوامر بشكل أفضل في etc/environment/، حيث سيتم حقن هذه المتغيرات في جميع المستخدمين جلسات العمل بفضل وحدة المصادقة القابلة للتوصيل (PAM) - حتى في حالة عدم تنفيذ برنامج shell.

٣.٣. نظام الملفات

٣.٣.١. نظام التسلسل الهرمي القياسي

كما هو الحال في توزيعات linux الأخرى، تم تنظيم kali linux بحيث يتوافق مع معيار *نظام الملفات الهرمي* (FHS)، مما يسمح لمستخدمي توزيعات linux الأخرى بالعثور على مساراتهم بسهولة في kali. يحدد FHS الغرض من كل مجلد، يتم وصف المجلدات كما يلي:

البرامج الأساسية binary	**/bin/**
نواة Kali Linux وملفات أخرى مطلوبة لعملية الإقلاع	**/boot/**
ملفات الجهاز device	**/dev/**
ملفات التكوين et cetera (بمعنى إلخ)	**/etc/**
ملفات المستخدم الشخصية	**/home/**
المكتبات الأساسية library	**/lib/**
نقاط وصل للأجهزة القابلة للإزالة، مثل: (USB, CD-Rom) وغيرها ...	**/media/***
نقاط الوصل المؤقتة mount	**/mnt/**
تطبيقات إضافية optional	**/opt/**
الملفات الشخصية للمسؤول (الجذر)	**/root/**
بيانات وقت التشغيل المتغيرة التي لا تبقى خلال عمليات إعادة التشغيل	**/run/**
برامج النظام system binary	**/sbin/**
البيانات المستخدمة من قبل الحوادم المستضافة على هذا النظام service	**/srv/**
ملفات مؤقتة (غالبا ما يتم إفراغ هذا المجلد عند الإقلاع) temporary	**/tmp/**

/usr/	التطبيقات (هذا المجلد ينقسم إلى **bin**، **sbin**، **lib** وفقًا لنفس المنطق كما في مجلد الجذر) علاوة على ذلك، **/usr/share/** يحتوي على بيانات مستقلة عن الهندسة المعمارية. من المفترض أن يستخدم مجلد **/usr/local/** من قبل المسؤول لتثبيت التطبيقات يدويًا دون الكتابة فوق الملفات التي يعالجها نظام الحزم (**dpkg**).
/var/	البيانات المتغيرة التي تعالجها الخوادم. يتضمن هذا ملفات السجل، قوائم الانتظار، التخزين المؤقت، وذاكرة التخزين المؤقت. variable
/proc/ and /sys/	خاصة بنواة Linux (وليست جزءًا من FHS). يتم استخدامها بواسطة النواة لتصدير البيانات إلى مساحة المستخدم.

٢.٣.٣. مجلد المستخدم الرئيسي

محتويات المجلد الرئيسي للمستخدم غير موحدة ولكن لا تزال هناك بعض المصطلحات الجديرة بالملاحظة. أحدهما هو أن المجلد الرئيسي للمستخدم غالبًا ما يشار إليه بواسطة التلدة ("~"). من

المفيد معرفة ذلك لأن مترجمي الأوامر يستبدلون التلدة تلقائيًا بالمجلد الصحيح (الذي يتم تخزينه في متغير بيئة **HOME**، وتكون قيمته المعتادة **/home/*user*/**).

تقليديًا، غالبًا ما يتم تخزين ملفات تكوين التطبيق مباشرةً في مجلدك الرئيسي، ولكن عادةً ما تبدأ أسماء الملفات بنقطة (على سبيل المثال، يخزن عميل البريد الإلكتروني **mutt** تكوينه في **~/.muttrc**). لاحظ أن أسماء الملفات التي تبدأ بنقطة هي مخفية افتراضيًا؛ الأمر **ls** يعرضهن فقط عند استخدام الخيار **-a** ويحتاج مديرو الملفات الرسومية إلى التهيئة بشكل صريح لعرض الملفات المخفية. تستخدم بعض البرامج أيضًا ملفات تكوين متعددة منظمة في مجلد واحد (على سبيل المثال، **~/.ssh/**). تستخدم بعض التطبيقات (مثل متصفح الويب Firefox) مجلدها أيضًا لتخزين ذاكرة التخزين المؤقت للبيانات التي تم تنزيلها. هذا يعني أن تلك المجلدات يمكن أن تستهلك الكثير من مساحة القرص.

ملفات الضبط هذه تخزن مباشرة في مجلدك الرئيسي، والتي يشار إليها مجتمعة في الغالب باسم *dotfiles*، قد انتشرت لفترة طويلة لدرجة أن هذه المجلدات يمكن تشويشها تمامًا. لحسن الحظ، نتج عن جهد بقيادة جماعية تحت مظلة FreeDesktop.org XDG مواصفات المجلدات الأساسية، وهي اتفاقية تهدف إلى تنظيف هذه الملفات والمجلدات. تنص هذه المواصفات على أنه ينبغي تخزين ملفات الضبط أو التكوين في **~/.config** وملفات ذاكرة التخزين المؤقت في **~/.cache** وملفات بيانات التطبيق في **~/.local** (أو المجلدات الفرعية الخاصة بها). هذه الاتفاقية تكتسب شعبيتها ببطء.

تحتوي أسطح المكتب الرسومية عادةً على اختصارات لعرض محتويات مجلد **~/Desktop/** (أو أيا كانت الترجمة المناسبة للأنظمة التي لم تتم تهيئتها باللغة الإنجليزية).

أخيرًا، يقوم نظام البريد الإلكتروني أحيانًا بتخزين رسائل البريد الإلكتروني الواردة في مجلد **~/Mail/**.

٣.٤. أوامر مفيدة

٣.٤.١. عرض وتعديل الملفات النصية

يقوم أمر `cat file` (المقصود به تسلسل (*concatenate*) الملفات لجهاز الإخراج القياسي) بقراءة الملف وعرض محتوياته على الـ(terminal). إذا كان الملف أكبر من أن يتم احتواؤه على الشاشة، فيمكنك استخدام قارىء الصفحات مثل **less** (أو **more**) لعرضه صفحة تلو الأخرى.

يبدأ أمر **editor** في محرر نصوص (مثل **vi** أو **nano**) ويسمح بإنشاء وتعديل وقراءة الملفات النصية. يمكن في بعض الأحيان إنشاء الملفات الأبسط مباشرة من مترجم الأوامر بفضل إعادة التوجيه: *command > file* ينشئ ملفًا باسم ملف يحتوي على مخرجات الأمر المحدد. يشبه *command >> file* إلا أنه يضيف إخراج الأمر في الملف بدلاً من الكتابة فوقه.

```
$echo "Kali rules!" > kali-rules.txt
$cat kali-rules.txt
    Kali rules!
$echo "Kali is the best!" >> kali-rules.txt
$cat kali-rules.txt
    Kali rules!
    Kali is the best!
```

٣.٤.٢. البحث عن الملفات وداخل الملفات

يبحث أمر *(المعايير)* *(المجلد)* **find** عن الملفات في التسلسل الهرمي ضمن المجلد وفقًا لعدة معايير. المعيار الأكثر استخدامًا هو *(اسم الملف)* **-name** الذي يسمح

بالبحث عن ملف بالاسم. يمكنك أيضًا استخدام أحرف البدل الشائعة مثل "*" في البحث عن اسم الملف.

```
$find /etc -name hosts
    /etc/hosts
    /etc/avahi/hosts
$find /etc -name "hosts"*
    /etc/hosts
    /etc/hosts.allow
    /etc/hosts.deny
    /etc/avahi/hosts
```

يبحث أمر **grep** في محتويات الملفات ويستخرج الأسطر المطابقة للتعبير العادي. تتيح إضافة الخيار **r-** إجراء بحث متكرر على جميع الملفات الموجودة في المجلد. يتيح لك هذا البحث عن ملف عندما تعرف جزءًا فقط من محتوياته.

٣.٤.٣. إدارة العمليات

يسرد أمر **ps aux** قائمة العمليات التي تعمل حاليًا ويساعد على تحديدها من خلال إظهار معرف PID الخاص بهم. بمجرد معرفة PID لعملية ما، يسمح لك الأمر:

```
kill -signal pid
```

بإرسال إشارة (إذا كنت تملك العملية). توجد عدة اشارات الأكثر استخدامًا هي **TERM** (طلب إنهاء بأمان) و **KILL** (قتل إجباري).

يمكن لمترجم الأوامر أيضًا تشغيل البرامج في الخلفية إذا كان الأمر يتبعه "&". باستخدام علامة الضم، تستأنف التحكم في الصدفة فورًا على الرغم من أن الأمر لا يزال قيد التشغيل (مخفي عن المشاهدة كعملية خلفية). يسرد أمر **jobs** العمليات التي تعمل في الخلفية، يؤدي تشغيل:

fg *%job-number* (للمقدمة)

إلى استعادة العملية للمقدمة. عندما يكون هناك أمر قيد التشغيل في المقدمة (إما بسبب بدء تشغيله بشكل طبيعي أو إعادته إلى المقدمة باستخدام **fg**)، فإن مجموعة المفاتيح Control + Z توقف العملية وتستأنف التحكم في سطر الأوامر. يمكن بعد ذلك إعادة تشغيل العملية في الخلفية باستخدام:

bg *%job-number* (للخلفية)

٤.٤.٣. إدارة الحقوق

Linux هو نظام متعدد المستخدمين، لذلك من الضروري توفير نظام أذونات للتحكم في مجموعة العمليات المعتمدة على الملفات والمجلدات، والتي تشمل جميع موارد النظام والأجهزة (على نظام

Unix، يتم تمثيل أي جهاز بواسطة ملف أو مجلد). هذا المبدأ شائع في جميع الأنظمة الشبيهة بيونكس.

كل ملف أو مجلد له أذونات محددة لثلاث فئات من المستخدمين:

- ❖ مالكها (يرمز له بـ **u**، اختصار لـ user).
- ❖ مجموعة المالكين (يرمز لهم بـ **g**، اختصار لـgroup)، والتي تمثل جميع أعضاء المجموعة.
- ❖ آخرين (يرمز لهم بـ **o**، اختصار لـ other).

وثلاثة أنواع من الحقوق:

- ❖ القراءة (يرمز لها بـ **r**، اختصار لـ read).
- ❖ الكتابة (أو التعديل، يرمز لها بـ **w**، اختصار لـ write).
- ❖ التنفيذ (يرمز له بـ **x**، اختصار لـ eXecute).

في حالة وجود ملف، يمكن فهم هذه الحقوق بسهولة: يتيح الوصول للقراءة: قراءة المحتوى (بما في ذلك النسخ)، ويسمح الوصول للكتابة: بتغييره، ويسمح الوصول للتنفيذ: بتشغيله (والذي لن يعمل إلا إذا كان برنامجًا).

أمن setuid و setgid التنفيذي

تسمح متغيرات البيئة بتخزين الإعدادات العامة للصدفة أو البرامج الأخرى المختلفة. فهي سياقية ولكن قابلة للتوريث. على سبيل المثال، تحتوي كل عملية على مجموعة متغيرات البيئة الخاصة بها (فهي سياقية). يمكن أن تقوم الصدفات، مثل صدفة تسجيل الدخول، بإعلان المتغيرات، والتي سيتم نقلها إلى البرامج الأخرى التي تنفذها (وهي قابلة للتوريث).

يمكن تعريف هذه المتغيرات على مستوى النظام في etc/profile/ أو لكل مستخدم في ملف التعريف profile./ ~ ولكن يتم وضع المتغيرات غير الخاصة بمترجمي سطر الأوامر بشكل أفضل في etc/environment/، حيث سيتم حقن هذه المتغيرات في جميع المستخدمين جلسات العمل بفضل وحدة المصادقة القابلة للتوصيل (PAM) - حتى في حالة عدم تنفيذ برنامج shell.

هناك نوعان من الحقوق المتعلقة بالملفات القابلة للتنفيذ: **setuid** و**setgid** (يرمز إليها بالحرف "s"). لاحظ أننا نتحدث كثيرًا عن bit، نظرًا لأن كل من هذه القيم المنطقية يمكن تمثيلها بالرقم ٠ أو ١. تسمح هذه الحقوق لأي مستخدم بتنفيذ البرنامج بحقوق المالك أو المجموعة، على التوالي. تتيح هذه الآلية الوصول إلى الميزات التي تتطلب أذونات مستوى أعلى من تلك التي عادة ما تكون لديك.

نظرًا لأن برنامج الجذر **setuid** يتم تشغيله بشكل منتظم تحت هوية المستخدم الفائق، فمن المهم للغاية التأكد من أنه آمن وموثوق. يمكن لأي مستخدم يدير تخريب برنامج جذر setuid لاستدعاء أمر من اختياره أن ينتحل هوية مستخدم الجذر ويحصل على جميع الحقوق على النظام. يبحث مختبروا الاختراق بشكل منتظم عن هذه الأنواع من الملفات عندما يتمكنون من الوصول إلى النظام كوسيلة لتصعيد امتيازاتهم.

يتم التعامل مع المجلد بشكل مختلف عن الملف. حق الوصول للقراءة يعطي حق الاطلاع على قائمة محتوياته (الملفات والمجلدات)؛ حق الكتابة يسمح بإنشاء أو حذف الملفات؛ وحق التنفيذ يسمح

بالعبور عبر المجلد للوصول إلى محتوياته (على سبيل المثال، باستخدام الأمر **cd**). أن تكون قادرًا على عبور مجلد دون القدرة على قراءته، يمنح المستخدم إذنًا بالوصول إلى الإدخالات الموجودة فيه والمعروفة بالاسم، ولكن لا يمكن العثور عليها دون معرفة اسمها الدقيق.

أمن مجلد setgid و sticky bit

setgid bit ينطبق أيضًا على المجلدات. أي عنصر تم إنشاؤه حديثًا في مثل هذه المجلدات يتم تلقائيًا تعيين مجموعة المالكين للمجلد الأصل، بدلاً من وراثة المجموعة الرئيسية للمنشئ كالمعتاد. لهذا السبب، لا يتعين عليك تغيير مجموعتك الرئيسية (باستخدام الأمر **newgrp**) عند العمل في شجرة ملفات مشتركة بين عدة مستخدمين لنفس المجموعة المخصصة.

sticky bit (التي يرمز لها بالحرف "**t**") هي إذن مفيد في المجلدات فقط. يستخدم بشكل خاص في المجلدات المؤقتة حيث يكون لكل شخص حق الوصول للكتابة (مثل **/tmp/**): فهو يقيد حذف الملفات بحيث يمكن فقط لمالكها أو مالك المجلد الأصل حذفها. في غياب ذلك، يمكن للجميع حذف ملفات المستخدمين الآخرين في **/tmp/**.

ثلاثة أوامر تتحكم في الأذونات المرتبطة بملف:

1. **chown** (المستخدم) (الملف)

لتغيير صاحب الملف.

> **نصحية لتغيير المستخدم والمجموعة**
>
> كثيرا ما تريد تغيير مجموعة الملف في نفس الوقت الذي تريد تغير المالك فيه. يحتوي الأمر **chown** على بنية خاصة بذلك:
>
> **chown** *user:group file*

لتغيير مجموعة المالكين:

2. **chgrp** *(المجموعة) (الملف)*

لتغيير أذونات الملف:

3. **chmod** *(الحقوق) (الملف)*

هناك طريقتان لتمثيل الحقوق، من بينها: **التمثيل الرمزي**: هو على الأرجح أسهل للفهم والتذكر. أنه يتكون من رموز الحروف المذكورة أعلاه. يمكنك تحديد الحقوق لكل فئة من فئات المستخدمين (**u / g / o**)، عن طريق تعيينها بشكل صريح (بـ =)، أو عن طريق إضافة (+)، أو طرح (-). وبالتالي فإن صيغة **u=rwx,g+rw,o-r**، تمنح المالك حقوق القراءة والكتابة والتنفيذ، وتضيف حقوق القراءة والكتابة لمجموعة المالكين، وتزيل حقوق القراءة للمستخدمين الآخرين. الحقوق التي لا تتغير عن طريق الجمع أو الطرح في مثل هذا الأمر تبقى غير معدلة. يعطي الحرف **a**، لجميع فئات المستخدمين الثلاثة، مثال: **a=rx** يمنح الفئات الثلاث نفس الحقوق (القراءة والتنفيذ، لكن ليس الكتابة).

يربط التمثيل الرقمي (الثماني) كل حق بقيمة:

- ٤: للقراءة.

❖ ٢: للكتابة.

❖ ١: للتنفيذ.

نحن نربط كل مجموعة من الحقوق بمجموع الأرقام الثلاثة، ويتم تعيين قيمة لكل فئة من فئات المستخدمين، بالترتيب المعتاد (المالك، المجموعة، آخرون).

على سبيل المثال، سيضع أمر *(الملف)* **chmod 754** الحقوق التالية: القراءة والكتابة والتنفيذ للمالك (حيث ٧=٤+٢+١)؛ القراءة والتنفيذ للمجموعة (حيث ٥=٤+١)؛ والآخرين القراءة فقط. الصفر 0 يعني عدم وجود حقوق؛ وبالتالي يسمح *(ملف)* **chmod 600** لأذونات القراءة والكتابة للمالك، ولا حقوق لأي شخص آخر. المجموعات الصحيحة الأكثر شيوعًا هي **755** للملفات القابلة للتنفيذ والمجلدات، و 644 لملفات البيانات.

لتمثيل الحقوق الخاصة، يمكنك اختصار أربعة أرقام لهذا الرقم وفقًا لنفس المبدأ، حيث تكون وحدات البت **setuid** و**setgid** و **sticky** هي ٤ و ٢ و ١ على التوالي. سيقوم الأمر **chmod 4754** بربط setuid bit مع الحقوق الموصوفة مسبقًا.

لاحظ أن استخدام الترميز الثماني يسمح لك فقط بتعيين جميع الحقوق في ملف واحد؛ **لا يمكنك استخدامه لإضافة حق جديد،** مثل الوصول للقراءة لمالك المجموعة، حيث يجب أن تأخذ في الاعتبار الحقوق الحالية وحساب القيمة العددية الجديدة المقابلة.

يتم استخدام التمثيل الثماني أيضًا مع أمر **umask**، والذي يُستخدم لتقييد الأذونات على الملفات التي تم إنشاؤها حديثًا. عندما يقوم أحد التطبيقات بإنشاء ملف، فإنه يعين أذونات إرشادية، مع العلم أن النظام يزيل تلقائيًا الحقوق المحددة باستخدام **umask**. اكتب **umask** في الصدفة. سترى قناعًا مثل **0022**. هذا مجرد تمثيل ثماني للحقوق المراد إزالتها بشكل منهجي (في هذه الحالة، حقوق الكتابة للمجموعة والمستخدمين الآخرين).

إذا أعطيتها قيمة ثمانية جديدة، فإن أمر **umask** يعدل القناع. المستخدمة في ملف تهيئة الصدفة (على سبيل المثال، **bash_profile.**/~) ، سيغير القناع الافتراضي لجلسات عملك بشكل فعال.

نصحية للعمليات مكررة

أحيانا، يتعين علينا تغيير الحقوق لشجرة الملفات بالكامل. جميع الأوامر المذكورة أعلاه لها خيار **R-** للعمل بشكل متكرر في المجلدات الفرعية.

يؤدي التمييز بين المجلدات والملفات أحيانًا إلى حدوث مشكلات في العمليات المتكررة. لهذا السبب تم تقديم حرف "**X**" في التمثيل الرمزي للحقوق. إنه يمثل حق التنفيذ الذي ينطبق فقط على المجلدات (وليس على الملفات التي تفتقر إلى هذا الحق). وبالتالي، فإن:

```
chmod -R a+X المجلد
```

سيضيف فقط حقوق التنفيذ لجميع فئات المستخدمين (a) لجميع المجلدات الفرعية والملفات التي لديها بالفعل فئة واحدة على الأقل من المستخدمين (حتى لو كان مالكها الوحيد) لديها حقوق تنفيذ .

٥.٤.٣. الحصول على معلومات النظام والسجلات

يعرض الأمر **free** معلومات عن الذاكرة العشوائية (RAM).

free disk (**df**): يعطي تقارير عن مساحة القرص المتوفرة على كل من الأقراص المثبتة في نظام الملفات. الخيار **h-** (للقراءة البشرية (*human readable*)) يحول الأحجام إلى وحدة أكثر وضوحًا (عادةً mebibytes أو gibibytes). بطريقة مماثلة، يدعم الأمر **free** خيارات **m-** و **g-**، ويعرض بياناته إما بـ mebibytes أو بـ gibibytes، على التوالي.

```
$free
              total        used        free      shared  buff/cache
available
Mem:        2052944      661232      621208       10520      770504
1359916
Swap:             0           0           0
$df
Filesystem     1K-blocks     Used Available Use% Mounted on
udev             1014584        0   1014584   0% /dev
tmpfs             205296     8940    196356   5% /run
/dev/vda1       30830588 11168116  18073328  39%/
tmpfs            1026472      456   1026016   1% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs            1026472        0   1026472   0% /sys/fs/cgroup
tmpfs             205296       36    205260   1% /run/user/132
tmpfs             205296       24    205272   1% /run/user/0
```

يعرض الأمر **id** هوية المستخدم الذي يدير الجلسة مع قائمة المجموعات التي ينتمي لها. نظرًا لأن الوصول إلى بعض الملفات أو الأجهزة قد يقتصر على أعضاء المجموعة، فقد يكون التحقق من عضوية المجموعة المتاحة مفيدًا.

```
$ id
uid=1000(buxy) gid=1000(buxy) groups=1000(buxy),27(sudo)
```

يُرجع الأمر **uname -a** سطرًا واحدًا يوثق اسم النواة (**linux**) واسم المضيف وإطلاق النواة وإصدار النواة ونوع الجهاز (والبنية، مثل: **x86_64**) واسم نظام التشغيل (**GNU/Linux**). عادةً ما يجب تضمين إخراج هذا الأمر في تقارير الأخطاء حيث إنه يحدد بوضوح النواة قيد الاستخدام ومنصة الأجهزة التي تعمل عليها.

```
$ uname -a
Linux kali-rolling 4.4.0-kali1-amd64 #1 SMP Debian 4.4.6-1kali1 (2016-03-18)
x86_64 GNU/Linux
```

توفر كل هذه الأوامر معلومات حول وقت التشغيل، ولكن غالبًا ما تحتاج إلى التحقق من السجلات لفهم ما حدث على جهازك. على وجه الخصوص، النواة تبعث الرسائل التي تخزنها في المخزن المؤقت الحلقي كلما حدث شيء مثير للاهتمام (مثل إدخال جهاز USB جديد، أو فشل تشغيل القرص الصلب، أو الكشف الأولي عن الأجهزة عند الإقلاع). يمكنك استرداد سجلات النواة باستخدام الأمر **dmesg**.

تقوم مجلة Systemd أيضًا بتخزين سجلات متعددة (مخرجات stdout/stderr من daemons، رسائل syslog، سجلات النواة) وتجعل من السهل طلبها باستخدام **journalctl**. بدون أي معلمات، فإنه يقوم فقط بعرض جميع السجلات المتاحة بطريقة التسلسل الزمني. باستخدام الخيار **r**- سيعكس الترتيب بحيث تظهر الرسائل الأحدث أولاً. باستخدام الخيار **f**- سوف

يطبع إدخالات السجل الجديد باستمرار حيث يتم إلحاقها بقاعدة البيانات الخاصة به. يمكن لخيار **u-** قصر الرسائل على تلك التي تنبعث من وحدة نظام معينة (على سبيل المثال:

journalctl -u ssh.service).

٦.٤.٣. استكشاف الهاردوير

تقوم النواة بتصدير العديد من التفاصيل حول الأجهزة المكتشفة من خلال نظام الملفات **/proc/** و **/sys/** الافتراضي. هناك عدة أدوات تلخص تلك التفاصيل. فيما بينها، يسرد **lspci** (في الحزمة pciutils) أجهزة PCI، ويسرد **lsusb** (في الحزمة usbutils) أجهزة USB، ويسرد **lspcmcia** (في الحزمة pcmciautils) بطاقات PCMCIA. هذه الأدوات مفيدة للغاية لتحديد النموذج الدقيق للجهاز. يتيح هذا التعريف أيضًا إجراء عمليات بحث أكثر دقة على الويب، مما يؤدي بدوره إلى المزيد من المستندات ذات الصلة. لاحظ أن حزم pciutils و usbutils مثبتة بالفعل على نظام Kali الأساسي ولكن يجب تثبيت pcmciautils بكتابة الأمر:

```
apt install pcmciautils
```

سنناقش المزيد حول تثبيت الحزم وإدارتها في فصل لاحق.

مثال ٣.١. مثال على المعلومات المخرجة من **lspci** و **lsusb**

```
$ lspci
[...]
00:02.1 Display controller: Intel Corporation Mobile 915GM/GMS/910GML Express
Graphics Controller (rev 03)
```

```
00:1c.0 PCI bridge: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) PCI
Express Port 1 (rev 03)
00:1d.0 USB Controller: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family)
USB UHCI #1 (rev 03)
[...]
01:00.0 Ethernet controller: Broadcom Corporation NetXtreme BCM5751 Gigabit
 Ethernet PCI Express (rev 01)
02:03.0 Network controller: Intel Corporation PRO/Wireless 2200BG Network
Connection (rev 05)
```

$ lsusb

```
Bus 005 Device 004: ID 413c:a005 Dell Computer Corp.
Bus 005 Device 008: ID 413c:9001 Dell Computer Corp.
Bus 005 Device 007: ID 045e:00dd Microsoft Corp.
Bus 005 Device 006: ID 046d:c03d Logitech, Inc.
[...]
Bus 002 Device 004: ID 413c:8103 Dell Computer Corp. Wireless 350 Bluetooth
```

تحتوي هذه البرامج على خيار **-v** يسرد معلومات أكثر تفصيلاً (لكنها عادةً غير ضرورية). أخيرًا، يسرد الأمر **lsdev** (في الحزمة procinfo) موارد الاتصال المستخدمة بواسطة الأجهزة.

برنامج **lshw** هو مزيج من البرامج المذكورة أعلاه ويعرض وصفًا طويلًا للأجهزة المكتشفة بطريقة هرمية. يجب إرفاق الإخراج الكامل لأي تقرير حول مشاكل دعم الأجهزة.

٥.٣. ملخص

في هذا الفصل، قمنا بجولة حول طبيعة Linux. ناقشنا مساحة النواة والمستخدم، واستعرضنا العديد من أوامر صدفة لينكس الشائعة، وناقشنا العمليات وكيفية إدارتها، واستعرضنا مفاهيم أمان المستخدم والمجموعة، وناقشنا نظام الملفات الهرمي FHS، وقمنا بجولة في بعض المجلدات والملفات الأكثر شيوعًا الموجودة في Kali Linux.

نصائح التلخيص:

غالبًا ما يتم استخدام Linux للإشارة إلى نظام تشغيل بالكامل، ولكن في الواقع لينكس هو نواة نظام التشغيل الذي يتم تشغيله بواسطة أداة محمل الإقلاع، والتي يتم تشغيلها هي نفسها بواسطة BIOS / UEFI.

تشير مساحة المستخدم إلى كل ما يحدث خارج النواة. من بين البرامج التي يتم تشغيلها في مساحة المستخدم، هناك العديد من الأدوات المساعدة الأساسية من مشروع GNU، ومعظمها يهدف إلى تشغيلها من سطر الأوامر (واجهة قائمة على النصوص تتيح لك إدخال الأوامر وتنفيذها، وعرض النتائج). تنفذ الصدفة الأوامر الخاصة بك داخل تلك الواجهة.

تتضمن الأوامر الشائعة:

- ❖ **pwd** (print working directory).
- ❖ **cd** (change directory).
- ❖ **ls** (listing).
- ❖ **mkdir** (make directory).
- ❖ **rmdir** (remove directory).

❖ **mv**، **rm** ، و **cp** (move, remove and copy).

❖ **cat** (concatenate).

❖ **more/less** (عرض الملفات صفحة تلو الأخرى).

❖ **editor** (بدء تشغيل محرر نصي).

❖ **find** (تحديد موقع ملف أو مجلد).

❖ **free** (عرض معلومات الذاكرة).

❖ **df** (disk free).

❖ **id** هوية المستخدم إلى جانب قائمة المجموعات التي ينتمي لها.

❖ **dmesg** (مراجعة سجلات النواة).

❖ **journalctl** (إظهار جميع السجلات المتاحة).

يمكنك التفاعل مع الجهاز على نظام Kali باستخدام العديد من الأوامر:

❖ **lspci** (قائمة أجهزة PCI).

❖ **lsusb** (قائمة أجهزة USB).

❖ **lspcmcia** (تسرد بطاقات PCMCIA).

العملية عبارة عن مثيل قيد التشغيل لبرنامج، والذي يتطلب ذاكرة لتخزين كل من البرنامج نفسه وبيانات التشغيل الخاصة به. يمكنك إدارة العمليات باستخدام أوامر مثل:

❖ **ps** (show processes).

❖ **kill** (kill processes).

❖ **bg** (send process to background).

❖ **fg** (bring background process to foreground).

❖ **jobs** (show background processes).

الأنظمة التي تشبه يونيكس متعددة المستخدمين. تدعم العديد من المستخدمين والمجموعات وتسمح بالتحكم في الإجراءات، بناءً على الأذونات. يمكنك إدارة حقوق الملفات والمجلدات باستخدام العديد من الأوامر، بما في ذلك:

❖ **chmod** (تغيير الأذونات).

❖ **chown** (تغيير المالك).

❖ **chgrp** (تغيير المجموعة).

كما هو الحال مع توزيعات Linux الأخرى، تم تنظيم Kali Linux بحيث يكون متوافقًا مع معيار نظام الملفات الهرمي (FHS)، مما يسمح للمستخدمين القادمين من توزيعات Linux الأخرى بالعثور على مساراتهم بسهولة في Kali.

بشكل تقليدي، يتم تخزين ملفات تكوين التطبيق ضمن مجلدك الرئيسي (home)، الملفات أو المجلدات المخفية تبدأ بنقطة.

الآن بعد أن أصبح لديك فكرة على أساسيات Linux، فلنقم بإنشاء Kali Linux وتشغيله.

التمرين الأول - الفصل الثالث

١. استخدم الأمر **file** لفحص بعض الأجهزة التي تم تصديرها بواسطة النواة في /dev/.
جرب **/dev/sda*** و **/dev/snd/***.

يرجى ملاحظة أنه إذا كنت تواجه مشكلة في الأوامر والمفاهيم الأساسية لنظام Linux، فيجب عليك التفكير بجدية في الحصول على دورة تدريبية مجانية على نظام Linux (مثل هذه الدورة التدريبية) قبل مواصلة تدريب Kali. تذكر! Kali Linux ليست لمبتدئي Linux!

التمرين الثاني للفصل الثالث: التحكم في العلميات

١. اكتب الأمر:

```
ping -i 10 localhost &
```

٢. بعدها، أكتب الأمر:

```
ping -i 10 127.0.0.1 &
```

٣. اعرض قائمة العلميات التي في الخلفية.

٤. انهِ عملية localhost

٥. الأن، أنهِ عملية ١٢٧,٠,٠,١

الإجابة:

يجب أن يكون الأمر كالاتي:

```
root@kali:~# ping -i 10 localhost &
[1] 3605
root@kali:~#  ping -i 10 127.0.0.1 &
[2] 3606
root@kali:~# jobs -l
[1]-  3605 Running                    ping -i 10 localhost &
[2]+  3606 Running                    ping -i 10 127.0.0.1 &
root@kali:~# kill %1
root@kali:~# jobs -l
[1]-  3605 Terminated                 ping -i 10 localhost
[2]+  3606 Running                    ping -i 10 127.0.0.1 &
oot@kali:~# kill %2
root@kali:~# jobs -l
[2]+  3606 Terminated                 ping -i 10 127.0.0.1
root@kali:~#
```

التمرين الثالث للفصل الثالث: البحث في وعن الملفات

١. جرب الأمر **dmesg** الذي يطبع رسائل النواة المخزنة، يحتوي إخراج هذا الأمر عادة على الرسائل التي تنتجها برامج تشغيل الأجهزة.

٢. استخدم الأمر **find** للعثور على ملف مسمى rockyou.txt.gz في نظام الملفات.

٣. استخدم الأمر **locate** لإيجاد ملف يسمى rockyou.txt.gz في نظام الملفات.

٤. أي أمر كان أسرع في البحث find أو locate، ولماذا؟

٥. يمكنك معرفة كيفية "الوقت" الأوامر لمعرفة مقدار الوقت الفعلي الذي تستغرقه الأوامر لإكمال؟

الإجابات:

١. إنه سهل جدا

```
dmesg | more
```

٢. أمر **find**:

```
find / -name rockyou.txt.gz
```

٣. أمر **locate**:

```
locate rockyou.txt.gz
```

٤. يجب أن يستغرق الأمر "**locate**" وقتًا أقل، بدلاً من البحث في نظام الملفات بالكامل عن ملف معين، يبحث الأمر "**locate**" في قاعدة بيانات تم تجميعها مسبقًا للملف المطلوب. في حال كنت تتساءل، يتم إنشاء قاعدة البيانات هذه كجزء من Kali ISO build، باستخدام الأمر "**updateb**". يمكنك استخدام الملف، ثم **zcat** لمعالجة هذا الملف.

٥. استخدم أمر **time** ^^!

التمرين الرابع للفصل الثالث: استكشاف الهاردوير

استخدام **lspci** و **dmesg** وأي أدوات مساعدة أخرى للتسجيل، اكتشف ما يلي حول مضيف Kali الخاص بك:

١. نوع وحدة المعالجة المركزية على مضيف Kali الخاص بك.

٢. نوع، وصنع وطراز محول إيثرنت.

٣. نوع وصنع ونموذج بطاقة الرسومات.

٤. نسخة من نواة قيد التشغيل.

٥. ذاكرة متاحة.

٦. مساحة القرص الحرة.

الإجابة:

```
1.    dmesg | grep CPU0
2.    lspci | grep Ethernet
3.    lspci -v -s `lspci | grep VGA | cut -f1 -d\ `
4.    uname -r
5.    free
6.    df
```

التمرين الخامس، للفصل الثالث: العمل على الهاردوير

١. قم بتوصيل أي جهاز USB بنظام الـ Kali الخاص بك.

٢. اعرف اسم هذا الجهاز.

٣. قم بتوصيل بطاقة USB لاسلكية بنظام الـ Kali.

٤. اعرف شرائح وطراز البطاقة اللاسلكية.

الإجابة:

انظر لمخرجات **lsusb** و **dmesg**.

غذاء الفكر:

١. ما نوع جهاز /dev/urandom؟

٢. أين يمكنني إيجاد ملفات ضبط الخوادم؟

الإجابة:

1. A character device: **ls -l /dev/random**

/* هذه الإجابة من الموقع، أما أنا كتبت file /dev/urandom */

2. /etc/

اختبار الشهادة للفصل الثالث

١. ما هو الحرف المستخدم لتمثيل المجلد الرئيسي للمستخدم؟

- ☐ ~
- ☐ !
- ☐ ?
- ☐ &

٢. ما هي الأدوات التي يمكن استخدامها للحصول على معلومات الملف؟ اختار كل ما ينطبق.

- ☐ pwd
- ☐ type
- ☐ echo
- ☐ which
- ☐ cat

٣. أي مما يلي ليس جهاز كتلة ولا حرف؟

- ☐ crw-rw—- 1 root tty 7, 132 Mar 21 08:30 vcsa4
- ☐ crw——- 1 root root 10, 63 Mar 21 08:30 vga_arbiter
- ☐ brw-rw—- 1 root disk 8, 0 Mar 21 08:30 sda
- ☐ drwxr-xr-x 2 root root 60 Mar 21 08:30 vfio

٤. كيف يمكن تمثيل أذونات الملف -r —w- بالرمز الثماني؟

- ☐ 751
- ☐ 420
- ☐ 411
- ☐ 110
- ☐ 200

٥. بناءً على قائمة الدليل الجزئي التالية، ما هي أذونات المستخدم لملف test؟

-r-x--x--- 1 user root 0 Mar 24 01:19 test

- ☐ بدون أذونات
- ☐ Read, Write, Execute
- ☐ Read, Execute
- ☐ Execute

٦. لديك وظيفتان تعملان في الخلفية. كيف تنهي أول وظيفة نفذتها؟

- ☐ CTRL-C
- ☐ `kill %1`
- ☐ `killall`
- ☐ `kill -signal pid`

٠٧ أي أمر لا يتحكم في الأذونات أو سمات المستخدم المرتبطة بالملف؟

- ☐ chperm
- ☐ `chgrp`
- ☐ `chmod`
- ☐ `chown`

٠٨ أي أمر يعرض هوية المستخدم الذي يدير الجلسة مع قائمة المجموعات التي ينتمي لها؟

- ☐ `cat /etc/passwd`
- ☐ `id`
- ☐ `who`
- ☐ `whoami`

٠٩ أي أمر يلخص أجهزة PCI من خلال أنظمة الملفات الافتراضية proc/ و sys/؟

- ☐ pci -v
- ☐ `cat /proc/pci`
- ☐ pciutil
- ☐ `lspci`

١٠. وفقًا لـ FHS، ما المجلد الذي يحتوي على ملفات السجل، وقوائم الانتظار، وملفات التخزين المؤقت، وبيانات ذاكرة التخزين المؤقت التي تتعامل معها ||الخوادم|| daemons؟

- ☐ /proc
- ☐ /var
- ☐ /sbin
- ☐ /bin

-----((الفصل الرابع))-----

تثبيت Kali Linux

في هذا الفصل، سوف نركز على عملية تثبيت Kali Linux. أولاً، سنناقش الحد الأدنى لمتطلبات التثبيت (الباب ٤.١. "الحد الأدنى لمتطلبات التثبيت") للتأكد من أن نظامك الحقيقي أو الافتراضي قد تم تهيئته بشكل جيد للتعامل مع نوع التثبيت الذي ستتبعه. بعد ذلك، سوف نمر بكل خطوة من خطوات عملية التثبيت (الباب ٤.٢. "التثبيت خطوة بخطوة على القرص الصلب") للتثبيت العادي، وكذلك للتثبيت الأكثر أمانًا الذي يتضمن نظام ملفات مشفر بالكامل.

سوف نناقش أيضًا مرحلة ما *قبل التثبيت* "`preseeding`"، والتي تسمح بالتثبيتات غير المراقبة (الباب ٤.٣. "التثبيتات الغير مراقبة") من خلال تقديم إجابات محددة مسبقًا على أسئلة التثبيت. سنبين لك أيضًا كيفية تثبيت `Kali Linux` على أجهزة ARM المختلفة (الباب ٤.٤. "تثبيتات ARM")، مما يوسع قدرات `Kali` إلى أبعد من سطح مكتب. أخيرًا، سوف نوضح لك ما يجب القيام به في حالة نادرة فشل التثبيت (الباب ٤.٥. "استكشاف أخطاء التثبيتات")، حتى تتمكن من حل المشكلة وإنهاء عملية تثبيت صعبة بنجاح.

١.٤. الحد الأدنى لمتطلبات التثبيت

تختلف متطلبات التثبيت لـ Kali Linux حسب ما تريد تثبيته. **الحد الأدنى**، يمكنك إعداد Kali كخادم Secure Shell (SSH) أساسي بدون سطح مكتب، باستخدام ذاكرة وصول عشوائي (RAM) لا تقل عن 128 MB (يوصى باستخدام 512 MB) و2 GB من مساحة القرص. **الحد الأعلى**، إذا اخترت تثبيت سطح مكتب GNOME الافتراضي وحزمة التعريف kali-linux-full، فيجب أن تحصل على 2048 MB على الأقل من ذاكرة الوصول العشوائي و20 GB من مساحة القرص.

إلى جانب متطلبات ذاكرة الوصول العشوائي والأقراص الصلبة، يحتاج الحاسوب لديك إلى وحدة المعالجة المركزية مدعومة على الأقل من بنيات amd64 أو i386 أو armel أو armhf أو arm64.

٢.٤. التثبيت خطوة بخطوة على القرص الصلب

في هذا الباب، نفترض أن لديك محرك أقراص USB أو قرص DVD قابلًا للإقلاع (راجع الباب ٤.١.٢. "نسخ الصورة على قرص DVD-ROM أو مفتاح USB" للحصول على تفاصيل حول كيفية إعداد محرك الأقراص هذا) وأنك قمت بالإقلاع منه لبدء عملية التثبيت.

١.٢.٤. تثبيت عادي

أولاً، سوف نلقي نظرة على تثبيت Kali القياسي، باستخدام نظام ملفات غير مشفر.

١.١.٢.٤. إقلاع وبدء التثبيت

بمجرد بدء BIOS في التشغيل من محرك أقراص USB أو DVD-ROM، تظهر قائمة أداة محمل الإقلاع لصورة لينكس، كما هو مبين في الشكل ١.٤. "شاشة الإقلاع". في هذه المرحلة، لم يتم تحميل نواة لينكس بعد؛ تتيح لك هذه القائمة اختيار نواة للإقلاع وإدخال معلمات اختيارية لنقلها إليه في هذه العملية.

للتثبيت القياسي، ما عليك سوى اختيار install أو Graphical Install (بمفاتيح الأسهم)، ثم اضغط على مفتاح **Enter** لبدء ما تبقى من عملية التثبيت.

يخفي كل إدخال قائمة سطر أوامر إقلاع محددًا، والذي يمكن تهيئته حسب الحاجة عن طريق الضغط على مفتاح **Tab** قبل التحقق من الإدخال والتشغيل.



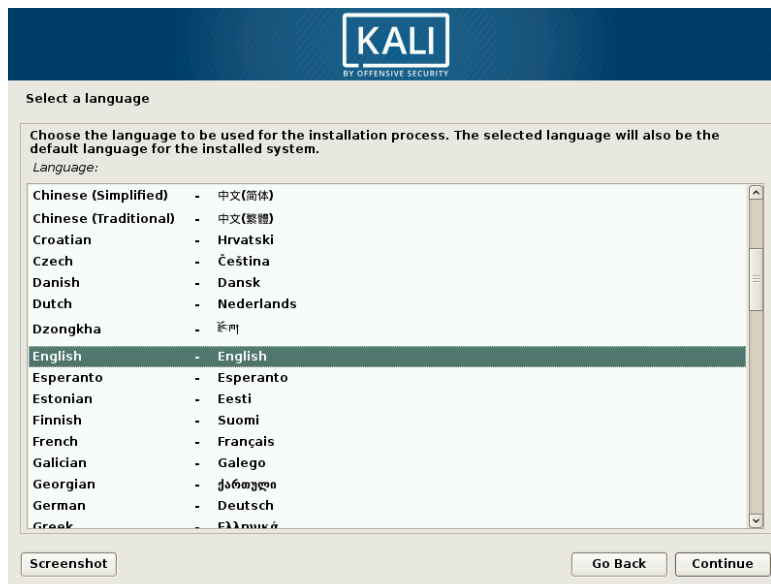
شكل ٤.١. شاشة الإقلاع

بمجرد الإقلاع، يرشدك برنامج التثبيت خطوة بخطوة خلال العملية. سوف نلقي نظرة على كل خطوة من هذه الخطوات بالتفصيل. سنغطي التثبيت من Kali Linux DVD-ROM قياسي؛ المثبتة من **mini.iso** قد تبدو مختلفة بعض الشيء. سنقوم أيضًا بتثبيت الوضع الرسومي، ولكن الفرق الوحيد من تثبيت وضع النص هو المظهر القديم.

٢.١.٢.٤. اختيار اللغة

كما هو مبين في الشكل ٢.٤. "اختيار اللغة"، يبدأ برنامج التثبيت باللغة الإنجليزية ولكن الخطوة الأولى تسمح لك باختيار اللغة التي سيتم استخدامها لبقية عملية التثبيت. يتم استخدام اختيار اللغة هذا أيضًا لتحديد الخيارات الافتراضية ذات الصلة في المراحل اللاحقة (لا سيما تخطيط لوحة المفاتيح).

> **التنقل باستخدام لوحة المفاتيح**
>
> تتطلب بعض الخطوات في عملية التثبيت إدخال المعلومات. تحتوي هذه الشاشات على العديد من الخانات التي تريد الإنتقال لها (خانة إدخال النص، وخانات الاختيار، وقائمة الخيارات، وأزرار الموافقة والإلغاء)، يسمح لك مفتاح **Tab** بالانتقال من خانة لإخرى. في وضع التثبيت الرسومي، يمكنك استخدام الماوس كما تفعل عادةً في سطح مكتب رسومي.



شكل ٢.٤. اختيار اللغة

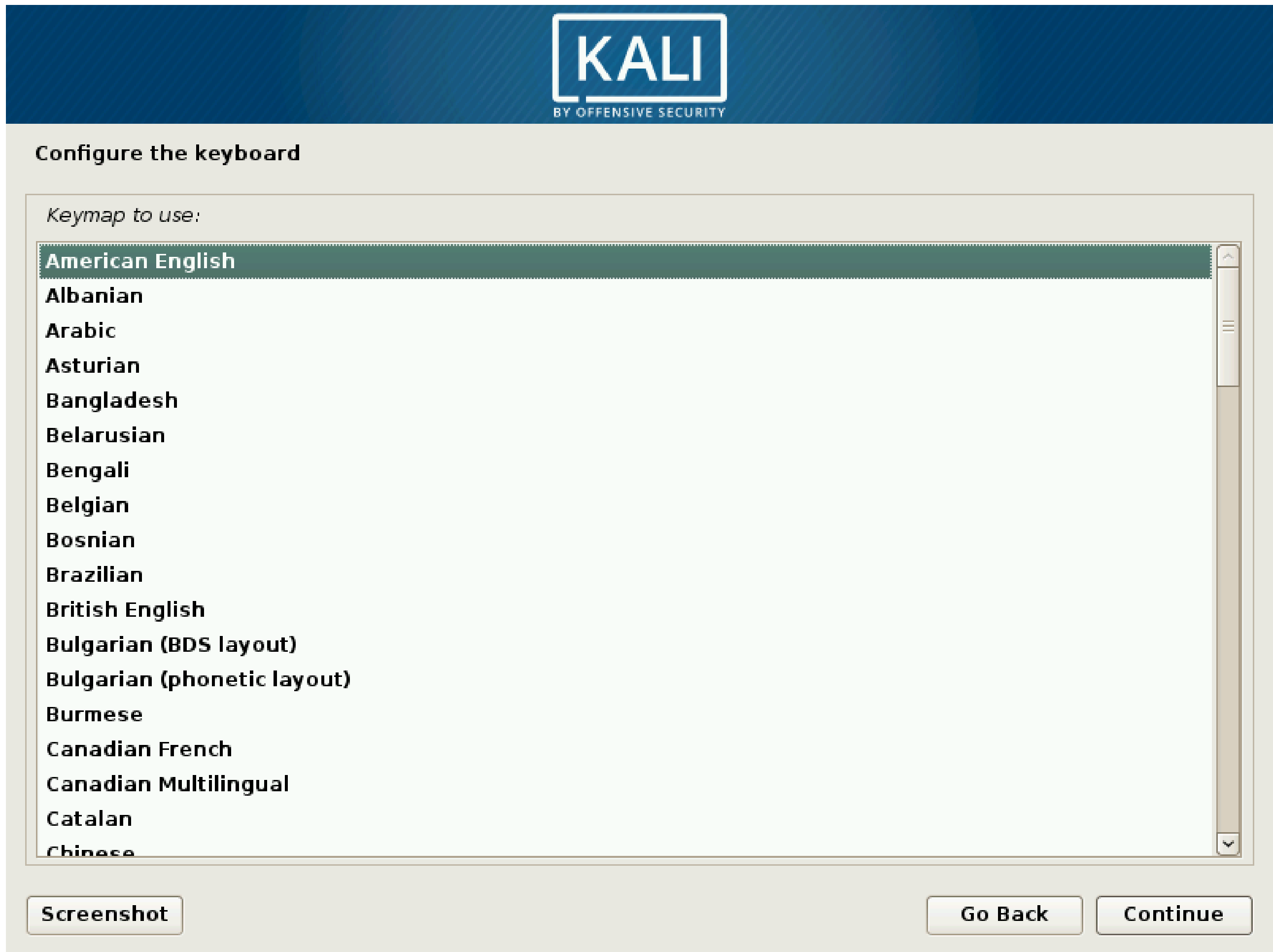
٣.١.٢.٤. اختيار البلد

تمثل الخطوة الثانية (الشكل ٣.٤. "اختيار البلد") في اختيار بلدك. بالإضافة إلى اللغة، تُمكّن هذه المعلومات برنامج التثبيت من تقديم تخطيط لوحة المفاتيح الأكثر ملاءمة. سيؤثر هذا أيضًا على تكوين المنطقة الزمنية. في الولايات المتحدة، تقترح لوحة مفاتيح QWERTY قياسية ويقدم المثبت اختيارًا للمناطق الزمنية المناسبة.

شكل ٣.٤. اختيار البلد

٤.١.٢.٤. اختيار تخطيط لوحة المفاتيح

تتوافق لوحة المفاتيح الإنجليزية الأمريكية المقترحة مع تخطيط QWERTY المعتاد كما هو موضح في الشكل ٤.٤ "اختيار تخطيط لوحة المفاتيح".



شكل ٤.٤. اختيار تخطيط لوحة المفاتيح

٥.١.٢.٤. التعرف على الهاردوير

غالبا تكون خطوة اكتشاف الأجهزة تلقائية بالكامل. يكشف المثبت عن أجهزتك ويحاول تحديد جهاز الإقلاع المستخدم للوصول إلى محتواه. يقوم بتحميل الوحدات المقابلة لمكونات الأجهزة المختلفة المكتشفة، ثم يقوم بوصل جهاز الإقلاع من أجل قراءته. تم تضمين الخطوات السابقة بالكامل في صورة الإقلاع المضمنة في جهاز الإقلاع، وهو ملف ذو حجم محدود ويتم تحميله في الذاكرة بواسطة أداة محمل الإقلاع عند التشغيل من جهاز الإقلاع.

٦.١.٢.٤. تحميل المكونات

مع توفر محتويات جهاز الإقلاع الآن، يقوم المثبت بتحميل جميع الملفات اللازمة لمتابعة عمله. يتضمن ذلك برامج تشغيل إضافية للأجهزة المتبقية (خاصة بطاقة الشبكة)، بالإضافة إلى جميع مكونات برنامج التثبيت.

٧.١.٢.٤. التحقق من هاردوير الشبكة

في هذه الخطوة، سيحاول المثبت تحديد بطاقة الشبكة تلقائيًا وتحميل الوحدة النمطية المقابلة. في حالة فشل الاكتشاف التلقائي، يمكنك تحديد الوحدة النمطية المراد تحميلها يدويًا. إذا فشل كل شيء آخر، يمكنك تحميل وحدة نمطية معينة من جهاز قابل للإزالة. عادة ما تكون هناك حاجة إلى هذا الحل الأخير فقط إذا لم يتم تضمين برنامج التشغيل المناسب في نواة لينكس القياسية، ولكنه متوفر في مكان آخر، مثل موقع الشركة المصنعة على الويب.

يجب أن تكون هذه الخطوة ناجحة تمامًا لعمليات تثبيت الشبكة (مثل تلك التي تمت عند التشغيل من **mini.iso**)، حيث يجب تحميل حزم دبيان من الشبكة.

٨.١.٢.٤. تكوين الشبكة

من أجل أتمتة العملية إلى أقصى حد ممكن، يحاول المثبت تكوين شبكة تلقائي باستخدام بروتوكول تكوين المضيف الحيوي "dynamic host configuration protocol" (DHCP) (لـ IPv4 و IPv6) (for IPv6) and ICMPv6's Neighbor Discovery Protocol ، كما هو مبين في الشكل ٤.٥. "التكوين التلقائي للشبكة ".



شكل ٤.٥. التكوين التلقائي للشبكة

في حالة فشل التكوين التلقائي، يقدم برنامج التثبيت المزيد من الخيارات: حاول مرة أخرى باستخدام تكوين DHCP عادي، أو حاول تكوين DHCP بالإعلان عن اسم الجهاز، أو قم بإعداد تكوين شبكة ثابت. يتطلب هذا الخيار الأخير عنوان IP وقناع شبكة فرعية وعنوان IP للبوابة واسم الجهاز واسم المجال.

التكوين بدون DHCP

> إذا كانت الشبكة المحلية مجهزة بخادم DHCP الذي لا ترغب في استخدامه لأنك تفضل تحديد عنوان IP ثابت للجهاز أثناء التثبيت، يمكنك إضافة خيار **netcfg/use_dhcp=false** عند التشغيل. تحتاج فقط إلى تحرير إدخال القائمة المطلوبة عن طريق الضغط على مفتاح **Tab** وإضافة الخيار المطلوب قبل الضغط على مفتاح **Enter**.

٩.١.٢.٤. كلمة السر للمستخدم الجذر

يطلب المثبت كلمة مرور (الشكل ٦.٤) لأنه يقوم تلقائيًا بإنشاء حساب جذر للمستخدم الفائق. يطلب المثبت أيضًا تأكيد كلمة المرور لمنع أي خطأ في الإدخال يصعب ضبطه لاحقًا.

شكل ٦.٤. كلمة مرور المستخدم الجذر

كلمة مرور المسؤول

يجب أن تكون كلمة مرور المستخدم الجذر طويلة (ثمانية أحرف أو أكثر) ولا يمكن تخمينها، لأن المهاجمين يستهدفون أجهزة الحاسوب والخوادم المتصلة بالإنترنت باستخدام أدوات آلية، ومحاولة تسجيل الدخول بكلمات مرور واضحة. يستفيد المهاجمون أحيانًا هجمات القاموس، وذلك باستخدام العديد من مجموعات الكلمات والأرقام وكلمات مرور. تجنب استخدام أسماء الأطفال أو الوالدين وتواريخ الميلاد، لأن هذه يسهل تخمينها.

تنطبق هذه الملاحظات بالتساوي على كلمات مرور المستخدمين الأخرين، لكن عواقب حساب مخترق تكون أقل حدة للمستخدمين دون حقوق إدارية.

إذا كنت تفتقر إلى الإلهام، فلا تتردد في استخدام مولد كلمات المرور، مثل **pwgen** (الموجود في الحزمة التي تحمل الاسم نفسه، والمضمنة بالفعل في تثبيت Kali الأساسي).

٤.٢.١.١٠. تكوين الساعة

إذا كانت الشبكة متوفرة، سيتم تحديث الساعة الداخلية للنظام من خادم بروتوكول وقت الشبكة (NTP). يعد هذا مفيدًا لأنه يضمن أن الطوابع الزمنية على السجلات ستكون صحيحة من الإقلاع الأول.

إذا امتد بلدك إلى مناطق زمنية متعددة، فسيُطلب منك تحديد المنطقة الزمنية التي تريد استخدامها، كما هو موضح في الشكل ٤.٧ "تحديد المنطقة الزمنية".

KALI
BY OFFENSIVE SECURITY
Configure the clock
If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).
Select your time zone:
Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa
Screenshot
Go Back
Continue

شكل ٤.٧. تحديد المنطقة الزمنية

٤.٢.١.١١. اكتشاف الأقراص والأجهزة الأخرى

تكتشف هذه الخطوة تلقائيًا محركات الأقراص الثابتة التي يمكن تثبيت Kali عليها، وسيتم تقديم كل منها في الخطوة التالية: التقسيم (partitioning).

٤.٢.١.١٢. التقسيم

التقسيم هو خطوة لا غنى عنها في التثبيت، والتي تتكون من تقسيم المساحة المتوفرة على محركات الأقراص الصلبة إلى أقسام منفصلة (*partitions*) وفقًا للوظيفة المقصودة للحاسوب وتلك الأقسام. يتضمن التقسيم أيضًا اختيار أنظمة الملفات المراد استخدامها. جميع هذه القرارات سيكون لها تأثير على الأداء، وأمن البيانات، وإدارة الخادم.

تعتبر خطوة التقسيم صعبة تقليدياً للمستخدمين الجدد. ومع ذلك، يجب تعريف أنظمة ملفات Linux والأقسام، بما في ذلك الذاكرة الافتراضية (أو أقسام المبادلة) لأنها تشكل أساس النظام. يمكن أن تصبح هذه المهمة معقدة إذا كنت قد قمت بالفعل بتثبيت نظام تشغيل آخر على الجهاز وتريد الحفاظ عليهما الاثنان. في هذه الحالة، يجب عليك التأكد من عدم تغيير أقسامهم، أو تغيير حجمهم إذا لزم الأمر دون التسبب في ضرر.

لفهم أوضاع التقسيم الأكثر شيوعًا (والأكثر بساطة)، يفضل معظم المستخدمين وضع الإرشاد *"Guided"* الذي يوصي بتكوينات القسم ويقدم اقتراحات في كل خطوة في الطريق. سيقدر المستخدمون الأكثر تقدماً الوضع اليدوي *"Manual"*، الذي يسمح بمزيد من التكوينات المتقدمة. يشارك كل وضع بعض القدرات.

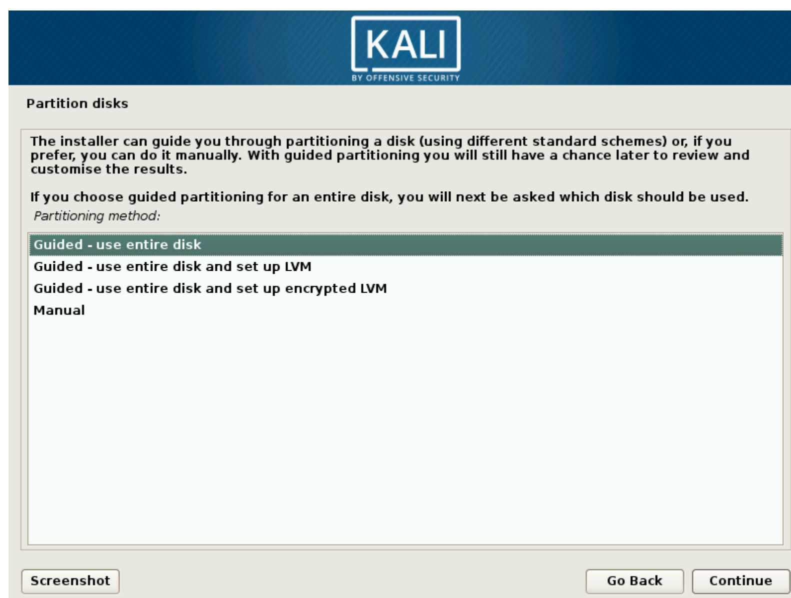
١.١٢.١.٢.٤. التقسيم الموجة

تعرض الشاشة الأولى في أداة التقسيم (الشكل ٨.٤ "اختيار وضع التقسيم") نقاط الدخول لأوضاع التقسيم الموجهة واليدوية. إن "إرشادات استخدام القرص بأكمله (Guided – use entire disk)" هو نظام التقسيم الأسهل والأكثر شيوعاً، والذي سيخصص قرصًا كاملًا لنظام Kali Linux.

يستخدم التحديدان التاليان (LVM) Logical Volume Manager لإعداد أقسام منطقية (بدلاً من المادية)، مشفرة اختيارياً. سنناقش LVM والتشفير لاحقًا في هذا الفصل.

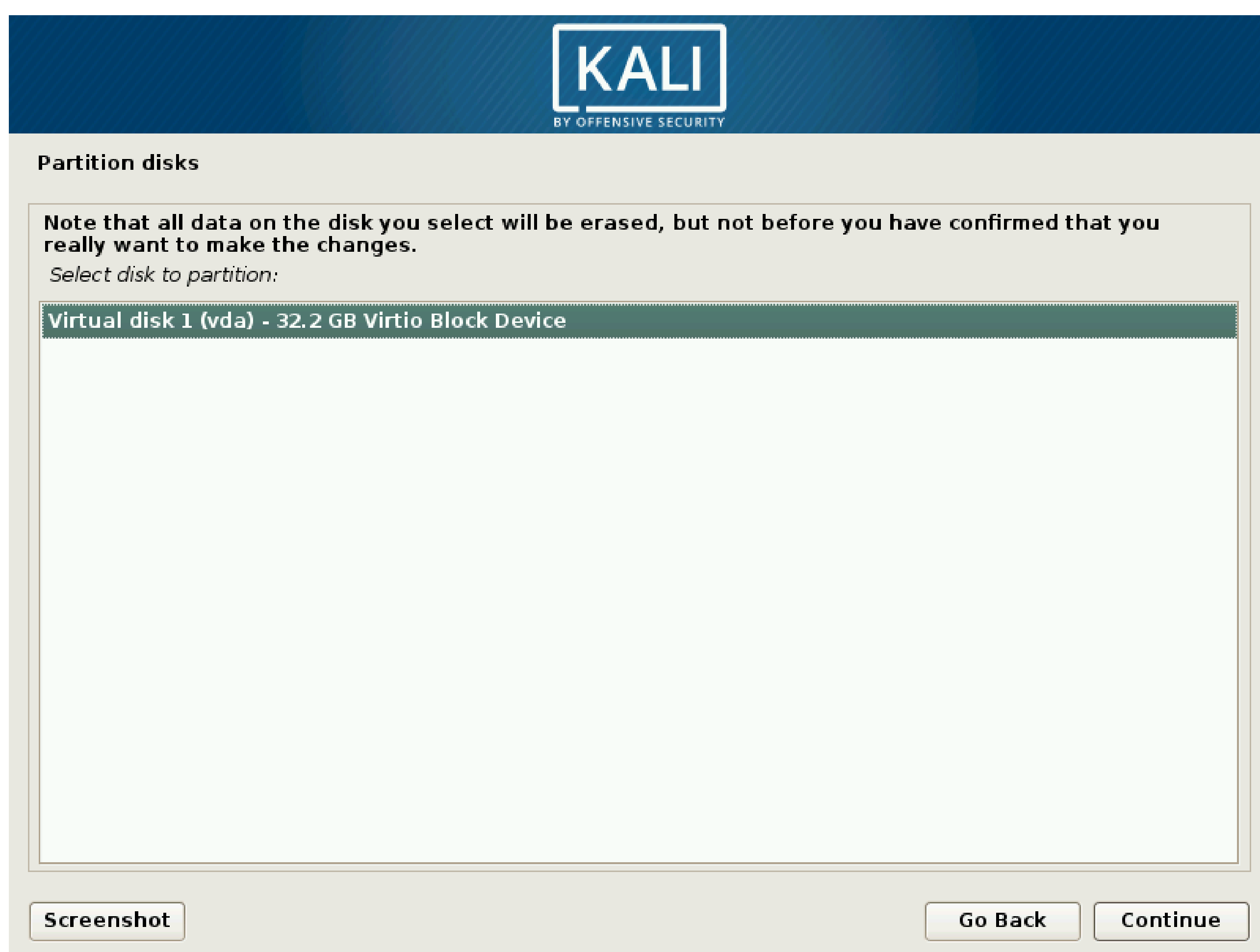
أخيرًا، يبدأ الخيار الأخير في التقسيم اليدوي، والذي يسمح بمزيد من مخططات التقسيم المتقدمة، مثل تثبيت Kali Linux إلى جانب أنظمة التشغيل الأخرى. سنناقش الوضع اليدوي في القسم التالي.

في هذا المثال، سنخصص قرصًا ثابتًا بالكامل لـ Kali، لذلك نختار " Guided – use entire disk " للمتابعة إلى الخطوة التالية.



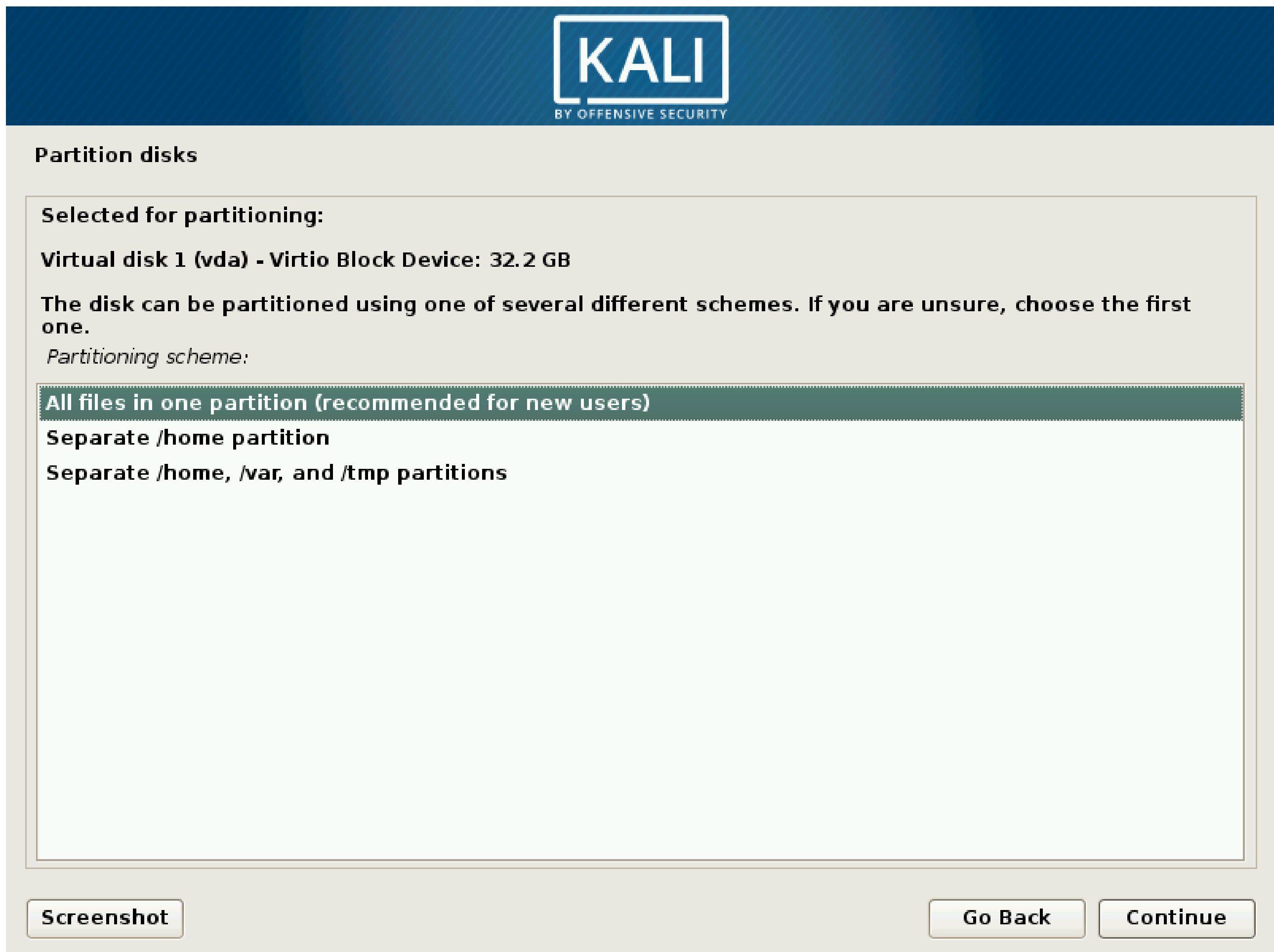
شكل ٨.٤. اختيار وضع التقسيم

تتيح لك الشاشة التالية (الموضحة في الشكل ٩.٤ "القرص المطلوب استخدامه للتقسيم الموجه") اختيار القرص الذي سيتم تثبيت Kali فيه عن طريق تحديد الإدخال المقابل (على سبيل المثال، "Virtual disk 1 (vda) - 32.2 GB Virtio Block Device"). بمجرد تحديده، سيستمر التقسيم الموجه. هذا الخيار سوف يمحو جميع البيانات الموجودة على هذا القرص، لذلك اختر بحكمة.



شكل ٩.٤. القرص المطلوب استخدامه للتقسيم الموجه

بعد ذلك، تقدم أداة التقسيم الموجهة ثلاث طرق تقسيم، والتي تتوافق مع استخدامات مختلفة، كما هو موضح في الشكل ٤.١٠، "تخصيص التقسيم الموجه".



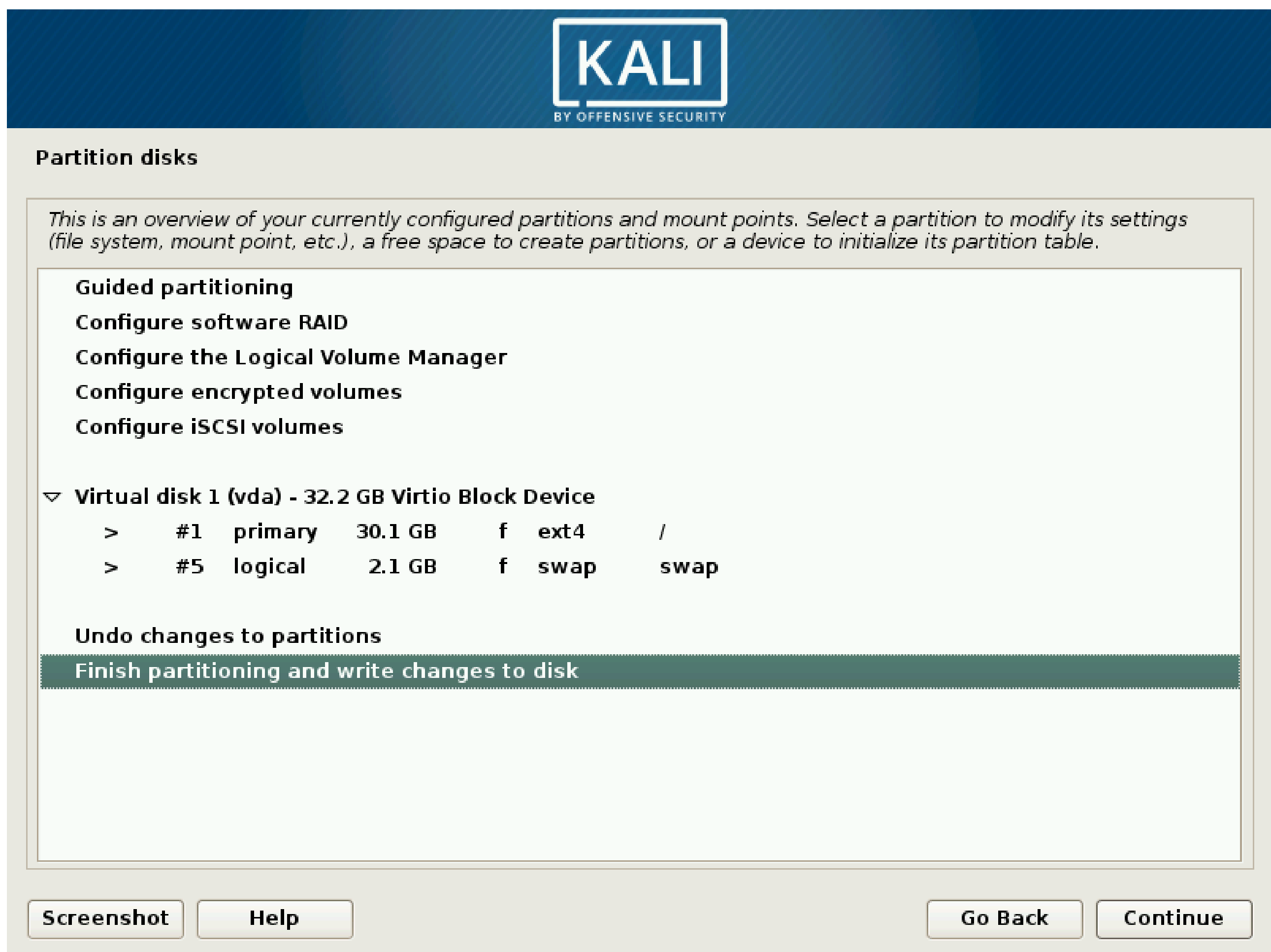
شكل ٤.١٠. تخصيص التقسيم الموجه

تسمى الطريقة الأولى "All files in one partition". يتم تخزين شجرة نظام Linux بالكامل في نظام ملفات واحد، يتوافق مع مجلد الجذر ("/"). يعمل نظام التقسيم البسيط والقوي هذا بشكل جيد على الأنظمة الشخصية أو أنظمة المستخدم الشخصية. على الرغم من الاسم، سيتم إنشاء قسمين بالفعل: الأول يضم النظام الكامل، والثاني الذاكرة الافتراضية (أو "المبادلة" "Swap").

تتشابه الطريقة الثانية، "Separate **/home/** partition"، ولكنها تقسم التسلسل الهرمي للملف إلى قسمين: قسم واحد يحتوي على نظام Linux (/)، والثاني يحتوي على "مجلدات home" (بمعنى بيانات المستخدم، في الملفات والمجلدات الفرعية متاح في **/home/**). من بين فوائد هذه الطريقة أنه من السهل الحفاظ على بيانات المستخدمين إذا كان عليك إعادة تثبيت النظام.

إن طريقة التقسيم الأخيرة، والتي تسمى "Separate **/home**, **/var**, and **/tmp** partitions"، مناسبة للخوادم وأنظمة المستخدمين المتعددين. يقسم شجرة الملفات إلى عدة أقسام: بالإضافة إلى أقسام الجذر **(/)** وحسابات المستخدمين (**/home/**)، كما أنه يحتوي على أقسام لبيانات برنامج الخادم (**/var/**)، والملفات المؤقتة (**/tmp/**). من فوائد هذه الطريقة أنه لا يمكن للمستخدمين قفل الخادم عن طريق استهلاك كل مساحة القرص الصلب المتاحة (يمكنهم فقط ملء **/tmp/** و **/home/**). في الوقت نفسه، لم تعد بيانات البرنامج الخفي (خاصة السجلات) تسد باقي النظام.

بعد اختيار نوع القسم، يقدم المثبت ملخصًا لاختياراتك على الشاشة كخريطة الأقسام (شكل ٤.١١ "التحقق من صحة التقسيم"). يمكنك تعديل كل قسم على حدة عن طريق تحديد قسم، على سبيل المثال: يمكنك اختيار نظام ملفات آخر إذا كان (*ext4*) غير مناسب. ومع ذلك، في معظم الحالات، يكون التقسيم المقترح معقولًا ويمكنك قبوله عن طريق اختيار " Finish partitioning and write changes to disk ". قد يستمر الأمر دون أن يقول ذلك، ولكن اختر بحكمة لأن هذا سيمحو محتويات القرص المحدد.



شكل ٤.١١. التحقق من صحة التقسيم

٢.١٢.١.٢.٤. التقسيم اليدوي

يتيح اختيار Manual في الشاشة الرئيسية "Partition disks" (شكل ٨.٤. "اختيار وضع التقسيم") مرونة أكبر، مما يسمح لك باختيار تكوينات أكثر تقدماً وإملاء غرض وحجم كل قسم على وجه التحديد. على سبيل المثال، يسمح لك هذا الوضع بتثبيت Kali إلى جانب أنظمة التشغيل الأخرى، وتمكين مجموعة متكررة قائمة على البرامج من الأقراص المستقلة " Redundant Array of Independent Disks"(RAID) لحماية البيانات من فشل القرص الصلب، وتغيير حجم الأقسام الموجودة بأمان دون فقدان البيانات، من بين أشياء أخرى.

إذا كنت مستخدمًا أقل خبرة يعمل على نظام يحتوي على بيانات حالية، فيرجى توخي الحذر الشديد مع طريقة الإعداد هذه، لأنه من السهل جدًا ارتكاب أخطاء قد تؤدي إلى فقدان البيانات.

تقليص قسم الوندوز

لتثبيت Kali Linux جنباً إلى جنب مع نظام تشغيل موجود (Windows أو غيره)، ستحتاج إلى مساحة متوفرة على القرص الصلب غير المستخدمة للأقسام المخصصة لـ Kali. في معظم الحالات، يعني هذا تقليص قسم موجود وإعادة استخدام المساحة المحررة.

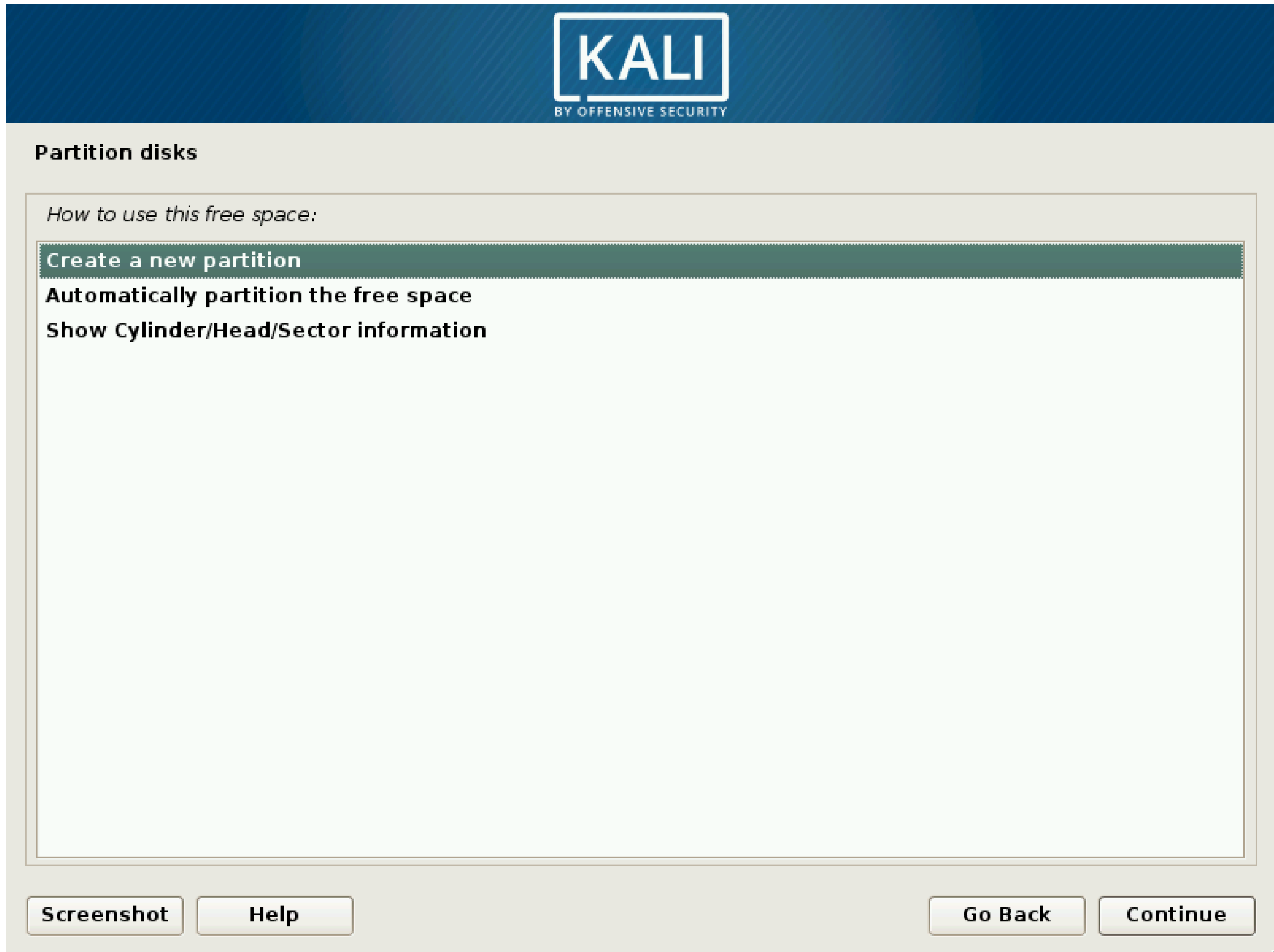
إذا كنت تستخدم وضع التقسيم اليدوي، فيمكن للمثبت تقليص قسم Windows بسهولة تامة. ما عليك سوى اختيار قسم Windows وإدخال حجمه الجديد (يعمل هذا مع كل من أقسام FAT وNTFS).

الشاشة الأولى في برنامج التثبيت اليدوي هي في الواقع نفس الشاشة الموضحة في الشكل ١١.٤. "التحقق من صحة التقسيم"، باستثناء أنه لا يتضمن أي أقسام جديدة لإنشائها. الأمر متروك لك لإضافة ذلك.

أولاً، سترى خيارًا لإدخال "Guided partitioning" متبوعًا بعدة خيارات تكوين. بعد ذلك، سيعرض برنامج التثبيت الأقراص المتوفرة وأقسامها وأي مساحة حرة ممكنة لم يتم تقسيمها بعد. يمكنك تحديد كل عنصر معروض والضغط على مفتاح **Enter** للتفاعل معه، كالمعتاد.

إذا كان القرص جديد تمامًا، فقد تضطر إلى إنشاء جدول أقسام. يمكنك القيام بذلك عن طريق اختيار القرص. بمجرد الانتهاء من ذلك، سترى مساحة حرة متوفرة داخل القرص.

للاستفادة من هذه المساحة الحرة، يجب عليك تحديدها وسيقدم لك المثبت طريقتين لإنشاء أقسام في تلك المساحة.



شكل ١٢.٤. إنشاء أقسام في المساحة الحرة

سيقوم الخيار الأول بإنشاء قسم واحد بالخصائص (بما في ذلك الحجم) من اختيارك. سيستخدم الإدخال الثاني كل المساحة الحرة وسيخلق أقساماً متعددة فيه بمساعدة معالج التقسيم الموجه (انظر القسم ١.١٢.١.٢.٤. "التقسيم الموجه"). يعد هذا الخيار ممتعاً بشكل خاص عندما تريد تثبيت Kali إلى جانب نظام تشغيل آخر ولكن عندما لا ترغب في إدارة تخطيط القسم بشكل دقيق. سيظهر الخيار الأخير أرقام cylinder/head/sector لبداية ونهاية المساحة الحرة.

عندما تختار "Create a new partition"، فسوف تدخل في سلسلة من تسلسل التقسيم اليدوي. بعد تحديد هذا الخيار، ستتم مطالبتك بحجم القسم. إذا كان القرص يستخدم جدول قسم MSDOS، فسيتم إعطاؤك خيار إنشاء قسم أساسي أو منطقي. (أشياء يجب معرفتها: لا يمكن أن

يكون لديك سوى أربعة أقسام أساسية ولكن هناك العديد من الأقسام المنطقية. القسم الذي يحتوي على boot/، تتبعه النواة، يجب أن يكون قسمًا أساسيًا، والأقسام المنطقية موجودة في قسم ممتد، يستهلك أحد الأقسام الأربعة الأساسية.) ثم سترى شاشة تكوين القسم العام:

KALI
BY OFFENSIVE SECURITY

Partition disks

You are editing partition #1 of Virtual disk 1 (vda). No existing file system was detected in this partition.
Partition settings:

Use as:	Ext4 journaling file system
Mount point:	/
Mount options:	defaults
Label:	none
Reserved blocks:	5%
Typical usage:	standard
Bootable flag:	off

Delete the partition
Done setting up the partition

Screenshot | Help | Go Back | Continue

شكل ٤.١٣. شاشة تكوين الأقسام

لتلخيص هذه الخطوة من التقسيم اليدوي، دعونا نلقي نظرة على ما يمكنك القيام به مع القسم الجديد. تستطيع:

❖ تنسيقه وتضمينه في شجرة الملفات عن طريق اختيار نقطة وصل.

نقطة الوصل: هو المجلد الذي سيضم محتويات نظام الملفات على القسم المحدد. وبالتالي، يُقصد عادةً بالقسم المُركب على **/home**/ أن يحتوي على بيانات المستخدم، بينما يُعرف "**/**" باسم جذر شجرة الملفات، وبالتالي فإن قسم الجذر هو الذي سيستضيف نظام `Kali` بالفعل.

❖ استخدامه كقسم المبادلة. عندما تفتقر نواة Linux إلى ذاكرة حرة كافية، فإنها تخزن أجزاء غير نشطة من ذاكرة الوصول العشوائي في قسم المبادلة الخاص على القرص الثابت. يجعل النظام الفرعي للذاكرة الافتراضية هذا شفافًا للتطبيقات. لمحاكاة الذاكرة الإضافية، يستخدم Windows ملف المبادلة (الترحيل) الموجود مباشرة في نظام الملفات. على العكس من ذلك، يستخدم Linux قسمًا مخصصًا لهذا الغرض، ومن هنا يأتي مصطلح قسم التبادل.

❖ جَعْلَهُ "physical volume for encryption" لحماية سرية البيانات على أقسام معينة. تتم أتمتة هذه الحالة في التقسيم الموجه. انظر القسم ٢.٢.٤."التثبيت على نظام ملفات مشفرة بالكامل" لمزيد من المعلومات.

❖ جعله "حجمًا فعليًا لـ LVM" (غير مشمول في هذا الكتاب). لاحظ أن هذه الميزة يتم استخدامها بواسطة التقسيم الموجه عند إعداد أقسام مشفرة.

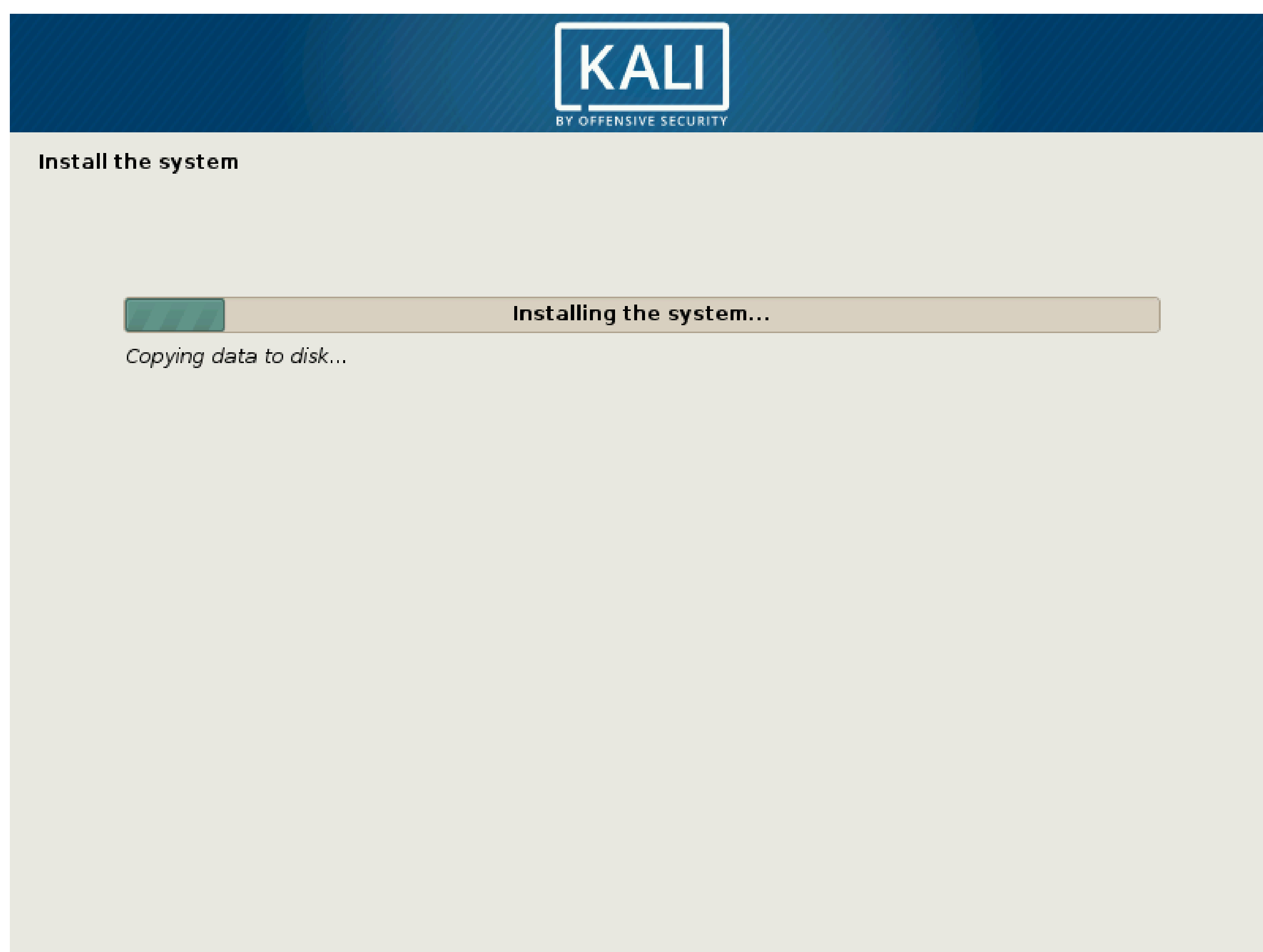
❖ استخدمه كجهاز RAID (غير مشمول في هذا الكتاب).

❖ اختيار عدم استخدام القسم واتركه دون تغيير.

عند الانتهاء، يمكنك إما الرجوع عن التقسيم اليدوي عن طريق اختيار "تراجع عن التغييرات إلى أقسام" أو كتابة التغييرات على القرص عن طريق تحديد "إنهاء التقسيم وكتابة التغييرات على القرص" من شاشة المثبت اليدوي (الشكل ١١.٤. "التحقق من صحة التقسيم").

١٣.١.٢.٤. نسخ الصورة المباشرة

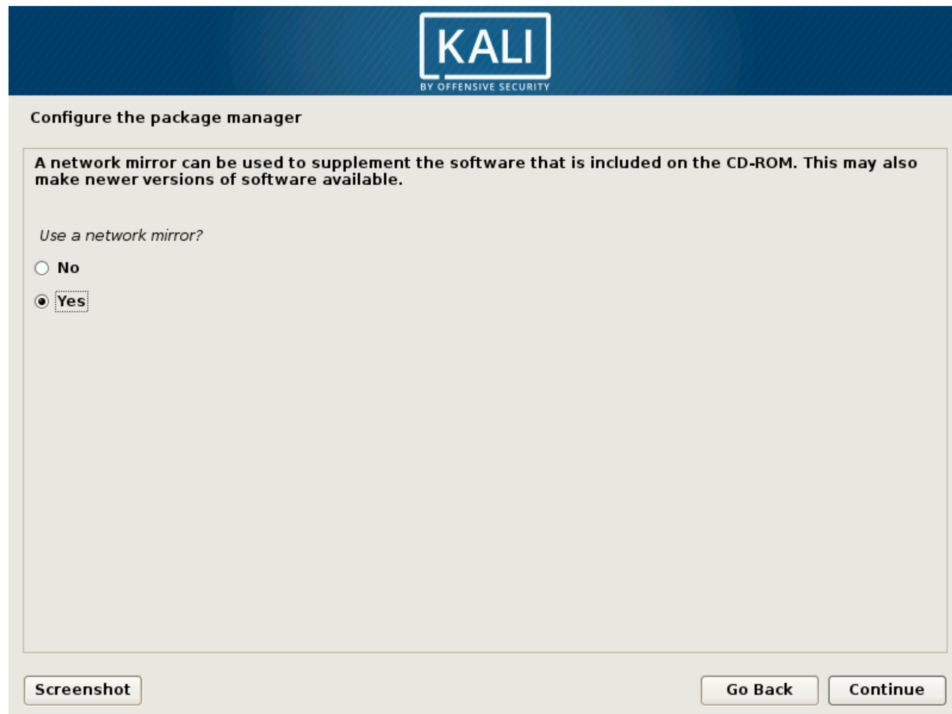
هذه الخطوة التالية، التي لا تتطلب أي تدخل من المستخدم، تنسخ محتويات الصورة المباشرة إلى نظام الملفات الهدف، كما هو موضح في الشكل ٤.١٤. "نسخ البيانات من الصورة المباشرة".



شكل ٤.١٤. نسخ البيانات من الصورة المباشرة

١٤.١.٢.٤. تكوين مدير الحزم (apt)

لكي تكون قادرًا على تثبيت برامج إضافية، يلزم تكوين APT وإخباره عن مكان حزم دبيان. في كالي، هذه الخطوة غير تفاعلية في أغلب الأحيان حيث نجبر المرآة على أن تكون **http.kali.org**. عليك فقط تأكيد ما إذا كنت تريد استخدام هذه النسخة المتطابقة (الشكل ١٥.٤. "استخدام مرآة شبكة؟"). إذا لم تستخدمها، فلن تتمكن من تثبيت حزم إضافية بـ **apt** إلا إذا قمت بتكوين مستودع الحزم لاحقًا.



شكل ١٥.٤. استخدام مرآة الشبكة؟

إذا كنت تريد استخدام نسخة متطابقة محلية بدلاً من **http.kali.org**، يمكنك تمرير اسمها في سطر أوامر النواة (في وقت الإقلاع) باستخدام بناء جملة مثل هذا:

```
mirror/http/hostname=my.own.mirror
```

أخيرًا، يقترح البرنامج استخدام وكيل *"proxy" HTTP* كما هو موضح في الشكل ١٦.٤. "استخدام وكيل HTTP". وكيل HTTP هو خادم يقوم بإعادة توجيه طلبات HTTP لمستخدمي الشبكة. يساعد في بعض الأحيان على تسريع التنزيلات عن طريق الاحتفاظ بنسخة من الملفات التي تم نقلها من خلالها (ثم نتحدث عن وكيل للتخزين المؤقت). في بعض الحالات، هي الوسيلة الوحيدة للوصول إلى خادم ويب خارجي؛ في مثل هذه الحالات، لن يتمكن المثبت من تنزيل حزم دبيان إلا إذا قمت بملء هذا الحقل بشكل صحيح أثناء التثبيت. إذا لم تقدم عنوانًا وكيلًا، فسيحاول المثبت الاتصال بالإنترنت مباشرةً.

KALI
BY OFFENSIVE SECURITY

Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):

Screenshot | Go Back | Continue

شكل ١٦.٤ استخدام وكيل http

بعد ذلك، سيتم تنزيل ملفي **Packages.xz** و**Sources.xz** تلقائيًا لتحديث قائمة الحزم المعترف بها من قِبل APT.

١٥.١.٢.٤. تثبيت محمل الإقلاع GRUB

محمل الإقلاع هو أول برنامج يتم تشغيله بواسطة BIOS. يقوم هذا البرنامج بتحميل نواة Linux في الذاكرة ثم تنفيذها. يقدم محمل الإقلاع غالبًا قائمة تتيح لك اختيار النواة المراد تحميلها أو نظام التشغيل للإقلاع.

نظراً لتفوقها التقني، فإن GRUB هو مُحّمل الإقلاع الافتراضي الذي تم تثبيته بواسطة Debian: إنه يعمل مع معظم أنظمة الملفات، وبالتالي لا يحتاج إلى تحديث بعد كل تثبيت نواة جديدة؛ لأنه يقرأ التكوين أثناء الإقلاع ويعثر على الموضع الدقيق من النواة الجديدة.

يجب تثبيت GRUB على سجل الإقلاع الرئيسي (MBR) ما لم يكن لديك بالفعل نظام لينكس آخر مثبت يعرف كيفية تشغيل Kali Linux. كما هو موضح في الشكل ١٧.٤. "تثبيت محمل الإقلاع GRUB على القرص الصلب" ، إن تعديل MBR سيجعل أنظمة التشغيل غير المعترف بها والتي تعتمد عليها غير قابلة للإقلاع حتى تقوم بإصلاح تكوين GRUB.



شكل ١٧.٤. تثبيت محمل الإقلاع GRUB على القرص الصلب

في هذه الخطوة (الشكل ١٨.٤. "الجهاز المطلوب لتثبيت محمل الإقلاع عليه")، يجب عليك تحديد الجهاز الذي سيتم تثبيت GRUB عليه. يجب أن يكون هذا هو محرك الإقلاع الحالي.



شكل ١٨.٤. الجهاز المطلوب لتثبيت محمل الإقلاع عليه

احترس: محمل الإقلاع والإقلاع المزدوج

تكتشف هذه المرحلة من عملية التثبيت أنظمة التشغيل المثبتة بالفعل على الحاسوب وستقوم تلقائيًا بإضافة الإدخالات المقابلة في قائمة الإقلاع. ومع ذلك، ليس كل برامج التثبيت تفعل هذا.

على وجه الخصوص، إذا قمت بتثبيت (أو إعادة تثبيت) Windows بعد ذلك، سيتم محو أداة محمل الإقلاع. سيظل نظام Kali موجود على محرك الأقراص الثابت؛ ولكن لن يكون من الممكن الوصول إليه من قائمة الإقلاع. سيكون عليك حينئذٍ بدء برنامج تثبيت Kali باستخدام المعلمة:

```
rescue/enable=true
```

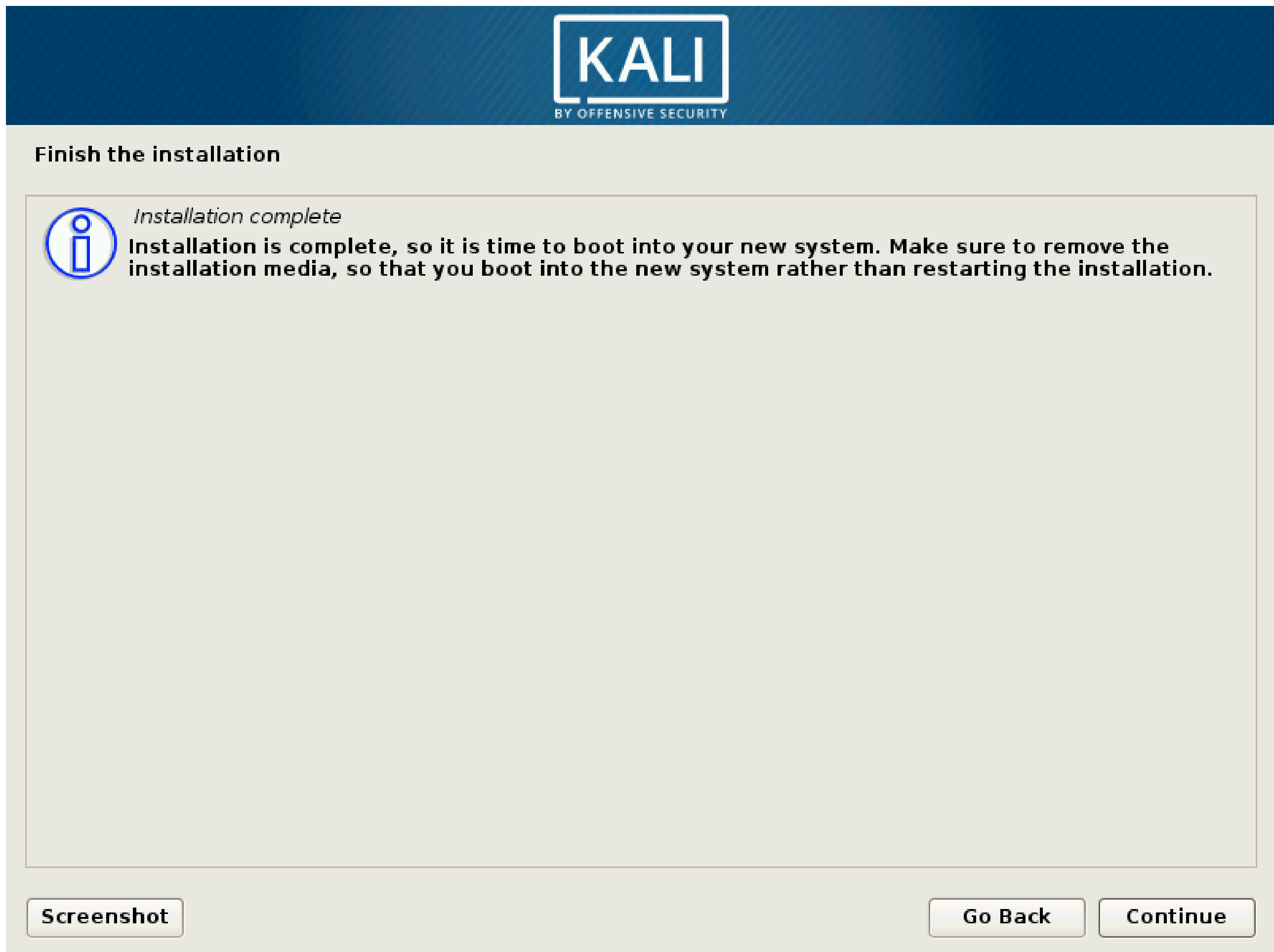
في سطر أوامر النواة لإعادة تثبيت أداة محمل الإقلاع. تم وصف هذه العملية بالتفصيل في دليل تثبيت ديبان.

http://www.debian.org/releases/stable/amd64/ch08s07.html

١٦.١.٢.٤. الانتهاء من التثبيت وإعادة التشغيل

الآن وبعد اكتمال التثبيت، يطلب منك البرنامج إزالة قرص DVD-ROM من القارئ (أو فصل محرك USB الخاص بك) حتى يتمكن جهاز الحاسوب من الإقلاع بنظام Kali الجديد الخاص بك بعد إعادة تشغيل برنامج التثبيت (الشكل ١٩.٤. "اكتمل التثبيت").

أخيرًا، سيقوم المثبت ببعض أعمال التنظيف، مثل إزالة الحزم الخاصة بإنشاء البيئة المباشرة.



شكل ١٩.٤. اكتمل التثبيت

٢.٢.٤. التثبيت بنظام ملفات مشفر بالكامل

لضمان سرية بياناتك، يمكنك إعداد أقسام مشفرة. سيؤدي ذلك إلى حماية بياناتك في حالة فقد الحاسوب المحمول أو القرص الصلب أو سرقته. يمكن لأداة التقسيم مساعدتك في هذه العملية، سواء في الوضع الإرشادي أو اليدوي.

سيجمع وضع التقسيم الموجه بين استخدام تقنيتين:

لتشفير الأقسام **L**inux **U**nified **K**ey **S**etup (LUKS)

لإدارة التخزين بشكل حيوي **L**ogical **V**olume **M**anagement (LVM)

يمكن أيضًا ضبط كلتا الميزتين وتكوينهما من خلال وضع التقسيم اليدوي.

١.٢.٢.٤. مقدمة في LVM

دعونا نناقش LVM أولاً. باستخدام مصطلحات LVM، القسم الافتراضي هو وحدة تخزين منطقية، والتي تعد جزءًا من مجموعة وحدات تخزين أو مجموعة من عدة وحدات تخزين فعلية. وحدات التخزين الفعلية هي أقسام حقيقية (أو أقسام افتراضية يتم تصديرها بواسطة أدوات تجريدية أخرى، مثل جهاز RAID للبرنامج أو قسم مشفر).

بفضل الافتقار إلى التمييز بين الأقسام "المادية" و "المنطقية"، يتيح لك LVM إنشاء أقسام "افتراضية" تمتد على عدة أقراص. الفوائد ذات شقين: لم يعد حجم الأقسام محددًا من قِبل الأقراص الفردية ولكن بواسطة حجمها التراكمي، ويمكنك تغيير حجم الأقسام الموجودة في أي وقت، مثل بعد إضافة قرص إضافي.

تعمل هذه التقنية بطريقة بسيطة للغاية: يتم تقسيم كل وحدة تخزين، سواء كانت مادية أو منطقية، إلى كتل من نفس الحجم، والتي يرتبط بها LVM. تؤدي إضافة قرص جديد إلى إنشاء وحدة

تخزين فعلية جديدة توفر كتلًا جديدة يمكن ربطها بأي مجموعة وحدات تخزين. يمكن لجميع الأقسام الموجودة في مجموعة مستوى الصوت الاستفادة الكاملة من المساحة المخصصة الإضافية.

٢.٢.٢.٤. مقدمة إلى LUKS

لحماية بياناتك، يمكنك إضافة طبقة تشفير أسفل نظام الملفات الذي تختاره. يستخدم Linux (وخاصة برنامج تشغيل *dm-crypt*) معين الجهاز لإنشاء القسم الافتراضي (الذي تكون محتوياته محمية) استنادًا إلى قسم أساسي يقوم بتخزين البيانات في نموذج مشفر (بفضل LUKS). يقيس LUKS تخزين البيانات المشفرة وكذلك معلومات التعريف التي تشير إلى خوارزميات التشفير المستخدمة.

تشفير قسم المبادلة

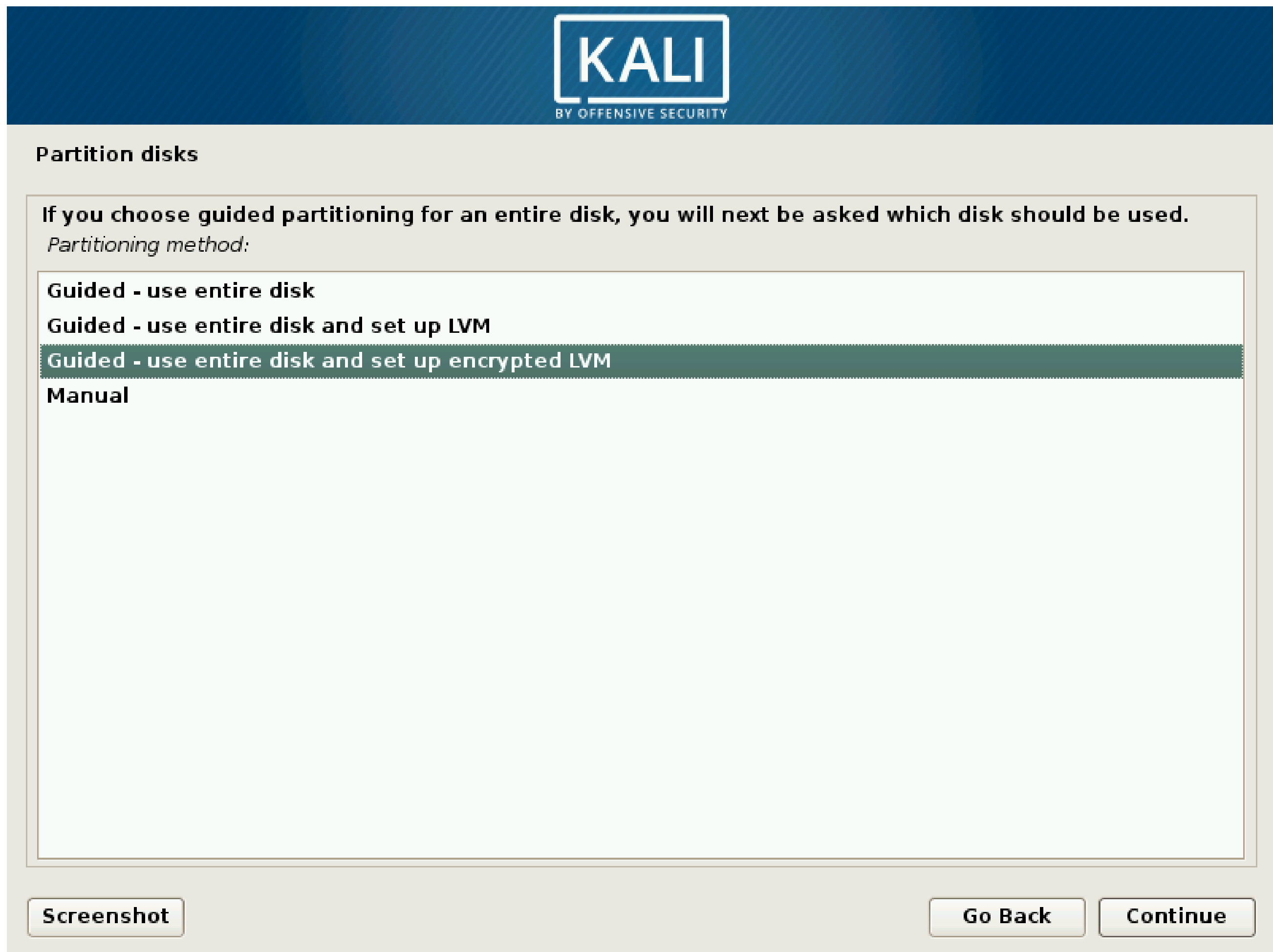
عند استخدام قسم مشفر، يتم تخزين مفتاح التشفير في الذاكرة (RAM)، وعند الإسبات، يقوم الحاسوب المحمول بنسخ المفتاح، إلى جانب محتويات أخرى من ذاكرة الوصول العشوائي، إلى قسم المبادلة للقرص الثابت. نظرًا لأن أي شخص لديه حق الوصول إلى ملف المبادلة (بما في ذلك فني أو لص) يمكنه استخراج المفتاح وفك تشفير بياناتك، فيجب حماية ملف المبادلة بالتشفير.

ولهذا السبب، سوف يحذرك برنامج التثبيت إذا حاولت استخدام قسم مشفر إلى جانب قسم تبديل غير مشفر. في سطر أوامر النواة لإعادة تثبيت أداة محمل الإقلاع. تم وصف هذه العملية بالتفصيل في دليل تثبيت ديبان.

http://www.debian.org/releases/stable/amd64/ch08s07.html

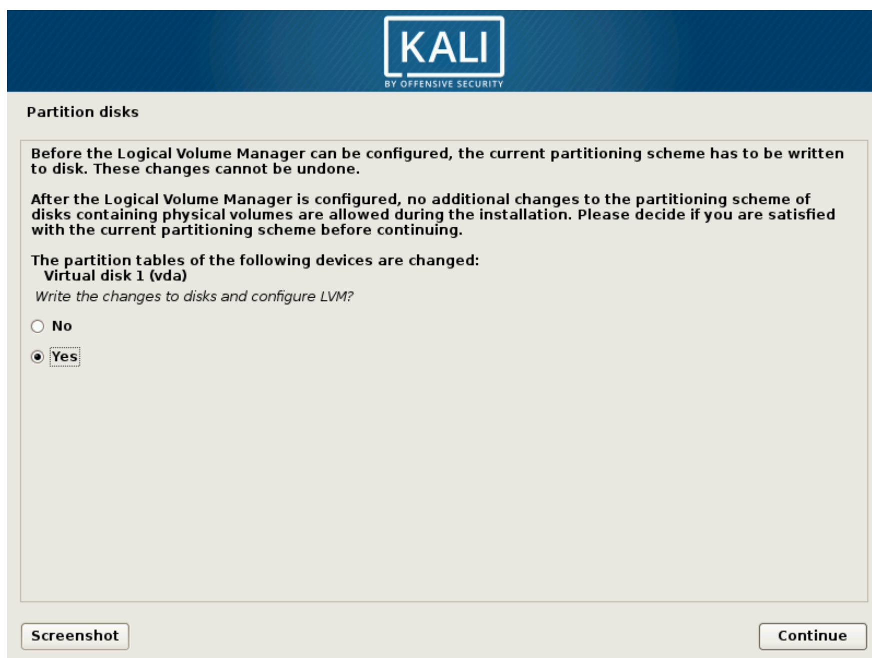
٣.٢.٢.٤. إعداد أقسام مشفرة

إن عملية تثبيت LVM المشفرة هي نفس عملية التثبيت القياسية باستثناء خطوة التقسيم (الشكل ٢٠.٤. "Guided Partitioning with Encrypted LVM") حيث ستختار بدلاً من ذلك "Guided – use entire disk and set up encrypted LVM". ستكون النتيجة نظامًا لا يمكن إقلاعه أو الوصول إليه حتى يتم توفير كلمة مرور التشفير. سيؤدي ذلك إلى تشفير وحماية البيانات الموجودة على القرص.



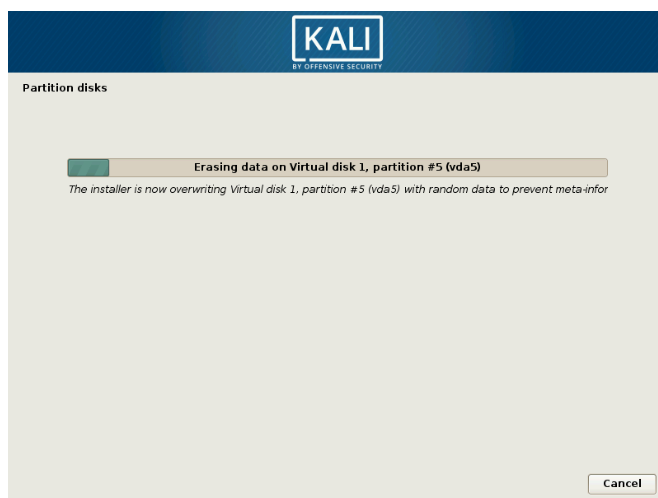
شكل ٢٠.٤. Guided Partitioning with Encrypted LVM

سيقوم مُثبّت التقسيم الموجه تلقائيًا بتعيين قسم فعلي لتخزين البيانات المشفرة، كما هو موضح في الشكل ٢١.٤ "تأكيد التغييرات على جدول الأقسام". في هذه المرحلة، سيقوم المثبت بتأكيد التغييرات قبل كتابتها على القرص.



شكل ٢١.٤. تأكيد التغييرات على جدول الأقسام

ثم يتم تهيئة هذا القسم الجديد ببيانات عشوائية، كما هو موضح في الشكل ٢٢.٤ "محو البيانات على القسم المشفر". هذا يجعل المناطق التي تحتوي على بيانات لا يمكن تمييزها عن المناطق غير المستخدمة، مما يجعل من الصعب اكتشاف البيانات المشفرة، ومن ثم مهاجمتها.



الشكل ٢٢.٤. محو البيانات على القسم المشفر

بعد ذلك، يطلب منك برنامج التثبيت إدخال كلمة مرور فك التشفير (الشكل ٢٣.٤."أدخل كلمة مرور فك التشفير"). لعرض محتويات القسم المشفر، ستحتاج إلى إدخال كلمة المرور هذه في كل مرة تقوم فيها بإعادة تشغيل النظام. لاحظ التحذير الموجود في برنامج التثبيت: سيكون نظامك المشفر قويًا بقدر قوة كلمة المرور هذه.

KALI
BY OFFENSIVE SECURITY

Partition disks

You need to choose a passphrase to encrypt Virtual disk 1, partition #5 (vda5).

The overall strength of the encryption depends strongly on this passphrase, so you should take care to choose a passphrase that is not easy to guess. It should not be a word or sentence found in dictionaries, or a phrase that could be easily associated with you.

A good passphrase will contain a mixture of letters, numbers and punctuation. Passphrases are recommended to have a length of 20 or more characters.

Encryption passphrase:

Show Password in Clear

Please enter the same passphrase again to verify that you have typed it correctly.

Re-enter passphrase to verify:

Show Password in Clear

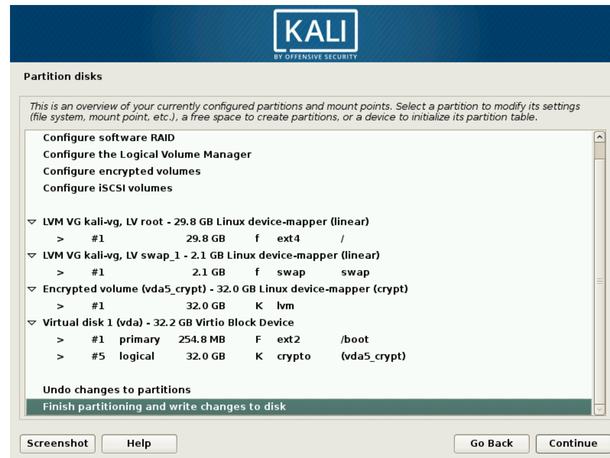
Screenshot | Go Back | Continue

شكل ٢٣.٤. ادخل كلمة مرور فك التشفير

تمتع أداة التقسيم الآن بالوصول إلى قسم افتراضي جديد يتم تخزين محتوياته مشفرة في القسم الفعلي الأساسي. نظرًا لأن LVM يستخدم هذا القسم الجديد كوحدة تخزين فعلية، يمكنه حماية عدة أقسام (أو وحدات تخزين منطقية LVM) باستخدام مفتاح التشفير نفسه، بما في ذلك قسم المبادلة (انظر الشريط الجانبي Encrypted Swap Partition). هنا، لا يتم استخدام LVM لتسهيل توسيع حجم التخزين، ولكن فقط من أجل توفير الراحة غير المباشرة التي تسمح بتقسيم قسم مشفر واحد إلى وحدات تخزين منطقية متعددة.

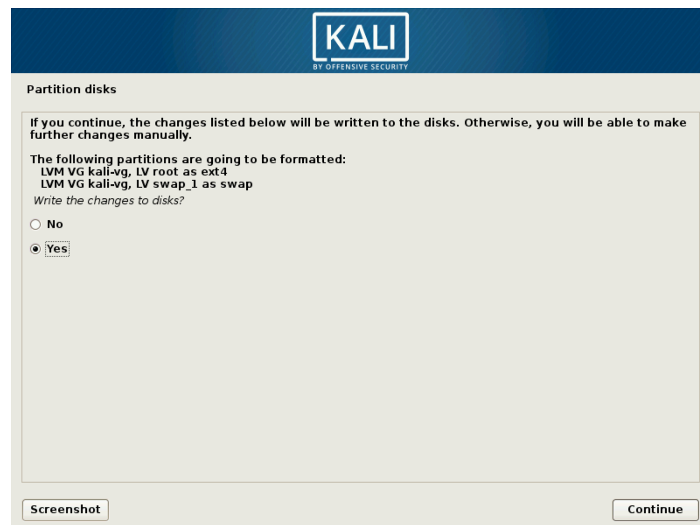
٤.٢.٢.٤. نهاية التقسيم الموجه باستخدام LVM المشفر

بعد ذلك، يتم عرض مخطط التقسيم الناتج (الشكل ٢٤.٤. "التحقق من صحة التقسيم لتثبيت LVM المشفر") حتى تتمكن من تعديل الإعدادات حسب الحاجة.



شكل ٢٤.٤. التحقق من صحة التقسيم لتثبيت LVM المشفر

أخيرًا، بعد التحقق من صحة إعداد القسم، تطلب الأداة تأكيد كتابة التغييرات على الأقراص، كما هو موضح في الشكل ٢٥.٤. "تأكيد الأقسام المراد تنسيقها".



شكل ٢٥.٤. تأكيد الأقسام المراد تنسيقها

أخيرًا، تستمر عملية التثبيت كالمعتاد كما هو موضح في القسم ١٤.١.٢.٤. "تكوين مدير الحزم (apt)".

٣.٤. التثبيت الغير مراقب

يعد مثبّتا دبيان وكالي نمطيًا للغاية: على المستوى الأساسي، ينفّذان فقط العديد من البرامج النصية (مجموعة في حزم صغيرة تسمى udeb — لـ µdeb أو micro-deb) واحدة تلو الأخرى. يعتمد كل برنامج نصي على debconf (راجع أداة **debconf**)، التي تتفاعل معك والمستخدم وتخزين معلمات التثبيت. لهذا السبب، يمكن أيضًا تثبيت برنامج التثبيت تلقائيًا من خلال أتمتة `debconf preseeding`، وهي دالة تتيح لك تقديم إجابات غير مراقبة لأسئلة التثبيت.

١.٣.٤. الإجابات المعدة مسبقا

هناك طرق متعددة لاستباق الإجابات على المثبت. كل أسلوب له مزاياه وعيوبه. بناءً على وقت حدوث عملية التغذية السابقة، تختلف الأسئلة التي يمكن إجراؤها.

١.١.٣.٤. بمعلمات الإقلاع

يمكنك أن تسبق أي سؤال مثبّت مع معلمات الإقلاع تنتهي في سطر أوامر النواة، يمكن الوصول إليها من خلال proc/cmdline/. ستتيح لك بعض أدوات تحميل الإقلاع تحرير هذه المعلمات بشكل تفاعلي (وهو أمر عملي لأغراض الاختبار)، ولكن إذا كنت تريد إجراء التغييرات، فسيتعين عليك تعديل تكوين أداة تحميل الإقلاع.

يمكنك استخدام المعرف الكامل لأسئلة `debconf` مباشرةً (مثل `debian-installer/language=en`) أو يمكنك استخدام الاختصارات للأسئلة الأكثر

شيوعًا (مثل `language=en` أو `hostname=duke`). انظر القائمة الكاملة للأسماء المستعارة -aliases- في دليل تثبيت دبيان.

لا يوجد أي قيود على الأسئلة التي يمكنك إجراؤها لأن معلمات الإقلاع متوفرة من بداية عملية التثبيت وتتم معالجتها في وقت مبكر جدًا. ومع ذلك، يقتصر عدد معلمات الإقلاع على 32 وعددًا من تلك المعلمات يتم استخدامها بالفعل افتراضيًا. من المهم أيضًا إدراك أن تغيير تكوين محمل الإقلاع يمكن أن يكون غير تافه في بعض الأحيان.

في القسم ٣.٩، "Building Custom Kali Live ISO Images"، ستتعلم أيضًا كيفية تعديل تكوين Isolinux عند إنشاء صورة Kali ISO الخاصة بك.

٢.١.٣.٤. بملف preseed في البداية

يمكنك إضافة ملف باسم preseed.cfg في جذر initrd الخاص بالمثبت (هذا هو initrd الذي يُستخدم لبدء المثبت). عادةً ما يتطلب ذلك إعادة إنشاء حزمة مصدر debian-installer لإنشاء إصدارات جديدة من initrd. ومع ذلك، يوفر التصميم المباشر طريقة مناسبة للقيام بذلك، وهو موضح بالتفصيل في القسم ٣.٩، "صور مخصصة بناء Kali Live ISO".

لا تحتوي هذه الطريقة أيضًا على أية قيود على الأسئلة التي يمكنك إجراؤها نظرًا لأن ملف preseed متاح فور بدء التشغيل. في كالي، استفدنا بالفعل من هذه الميزة لتخصيص سلوك مثبت دبيان الرسمي.

٣.١.٣.٤. مع ملف Preseed في Boot Media

يمكنك إضافة ملف مسبق على وسائط الإقلاع (CD أو مفتاح USB)؛ يحدث ذلك قبل بدء الوسائط، مما يعني مباشرة بعد الأسئلة حول تخطيط اللغة ولوحة المفاتيح. يمكن استخدام معلمة الإقلاع preseed/file للإشارة إلى موقع ملف preseed (على سبيل المثال، cdrom/preseed.cfg/ عند التثبيت من قرص مضغوط أو hd-media/preseed.cfg/ عند التثبيت من مفتاح USB).

لا يجوز لك تقديم إجابات على خيارات اللغة والبلد حيث يتم تحميل ملف preseeding لاحقًا في العملية، بمجرد تحميل برامج تشغيل الأجهزة. على الجانب الإيجابي، تجعل عملية الإنشاء المباشر من السهل وضع ملف إضافي في صور ISO التي تم إنشاؤها (انظر القسم ٣.٩، "صور مخصصة بناء Kali Live ISO").

٤.١.٣.٤. بملف preseed محمل من الشبكة

يمكنك إتاحة ملف مسبق على الشبكة من خلال خادم ويب وإخبار المثبت بتنزيل هذا الملف قبل إضافة معلمة الإقلاع:

preseed/url=http: //server/preseed.cfg أو باستخدام عنوان url المستعار "alias.")

ومع ذلك، عند استخدام هذه الطريقة، تذكر أنه يجب تكوين الشبكة أولاً. هذا يعني أن أسئلة debconf المتعلقة بالشبكة (خاصة اسم المضيف واسم المجال) وجميع الأسئلة السابقة (مثل اللغة والبلد) لا يمكن إعطاؤها بهذه الطريقة. غالبًا ما يتم استخدام هذه الطريقة مع معلمات الإقلاع التي تسبق هذه الأسئلة المحددة.

طريقة التجميع هذه هي الأكثر مرونة حيث يمكنك تغيير تكوين التثبيت دون تغيير وسائط التثبيت.

تأخير أسئلة اللغة، البلد، لوحة المفاتيح

للتغلب على قيود عدم القدرة على الافتراض على أسئلة اللغة والدولة ولوحة المفاتيح، يمكنك إضافة معلمة الإقلاع `auto-install/enable=true` (أو `auto = true`). باستخدام هذا الخيار، سيتم طرح الأسئلة لاحقًا في هذه العملية، بعد تهيئة الشبكة، وبالتالي بعد تنزيل الملف الرئيسي.

الجانب السلبي هو أن الخطوات الأولى (لا سيما تكوين الشبكة) ستحدث دائمًا باللغة الإنجليزية، وإذا كانت هناك أخطاء، فسيتعين على المستخدم العمل من خلال شاشات باللغة الإنجليزية (مع تكوين لوحة مفاتيح في(QWERTY).

4.3.2. إنشاء ملفpreseed

ملف preseed هو ملف نصي عادي يحتوي فيه كل سطر على إجابة سؤال Debconf واحد. يتم تقسيم السطر لأربعة حقول مفصولة بمسافة بيضاء (مسافات أو tabs). على سبيل المثال،

```
d-i mirror/suite string kali-rolling:
```

❖ يشير الحقل الأول إلى صاحب السؤال. على سبيل المثال، يتم استخدام "d-i" للأسئلة المتعلقة بالمثبت (installer) || لعله اختصار لـ "debian installer"||. قد ترى أيضًا اسم حزمة للأسئلة الواردة من حزم دبيان (كما في هذا المثال: atftpd atftpd / use_inetd boolean false).

❖ الحقل الثاني هو معرف للسؤال.

❖ يسرد الحقل الثالث نوع السؤال.

❖ يحتوي الحقل الرابع والأخير على قيمة الإجابة المتوقعة. لاحظ أنه يجب فصله عن الحقل الثالث بمسافة واحدة؛ تعتبر أحرف المسافات الإضافية جزءًا من القيمة.

إن أبسط طريقة لكتابة ملف preseed هي تثبيت النظام يدويًا. ثم سيقدم الأمر:

```
debconf-get-selections - installer
```

الإجابات التي قدمتها للمثبت. يمكنك الحصول على إجابات موجهة إلى الحزم الأخرى باستخدام:

```
debconf-get-selections
```

ومع ذلك، فإن الحل الأنظف هو كتابة الملف يدويًا، بدءًا من المثال ثم المرور بالوثائق. باستخدام هذا النهج، يمكن فقط توقع الأسئلة التي تحتاج إلى تجاوز الإجابة الافتراضية. قدّم معلمة الإقلاع:

```
priority=critical
```

لـ (مرشد ديبيان) Instruct Debconf إلى طرح الأسئلة المهمة فقط، واستخدام الإجابة الافتراضية للباقي.

ملحق دليل التثبيت

يحتوي دليل تثبيت دبيان، المتاح عبر الإنترنت، على وثائق تفصيلية حول استخدام ملف preseed في الملحق. كما يشمل أيضا ملف مفصل وتعليقات بسيطة، يمكن أن يكون بمثابة قاعدة للتخصيصات المحلية.

https://www.debian.org/releases/stable/amd64/apb.html

https://www.debian.org/releases/stable/example-preseed.txt

لاحظ أن الروابط السابقة توثق الإصدار المستقر من دبيان وأن كالي يستخدم الإصدار (Debian testing)، لذا فقد تواجه اختلافات بسيطة. يمكنك أيضًا الرجوع إلى دليل التثبيت المستضاف على موقع مشروع مثبت دبيان (Debian-installer). قد يكون أكثر حداثة.

٤.٤. تثبيت على أجهزة ARM

يعمل Kali Linux على مجموعة متنوعة من الأجهزة المستندة إلى ARM (أجهزة الحاسوب المحمولة وأجهزة الحاسوب المضمنة ولوحات المطورين، على سبيل المثال) ولكن لا يمكنك استخدام مثبت Kali التقليدي على هذه الأجهزة نظراً لأنها غالبًا ما تكون لها متطلبات محددة فيما يتعلق بتكوين النواة أو محمل الإقلاع.

لجعل هذه الأجهزة في متناول مستخدمي Kali، قامت Offensive Security بتطوير نصوص برمجية لإنشاء صور قرص جاهزة للاستخدام لأجهزة ARM المختلفة. توفر هذه الصور للتنزيل على موقعها على الويب:

https://www.offensive-security.com/kali-linux-arm-images/

نظراً لأن هذه الصور متاحة، فإن مهمتك في تثبيت Kali على جهاز ARM بسيطة لحد كبير. وهنا الخطوات الأساسية:

- قم بتنزيل الصورة لجهاز ARM الخاص بك وتأكد من أن المجموع الاختباري يطابق الموجود على موقع الويب (انظر القسم ٣.١.٢، "التحقق من النزاهة والأصالة" للحصول على توضيحات حول كيفية القيام بذلك). لاحظ أن الصور عادةً ما تكون مضغوطة بتنسيق xz، تأكد من إلغاء ضغطها باستخدام **unxz**.
- اعتماداً على فتحة توسيع التخزين المتاحة على أجهزة ARM الخاص بك، احصل على بطاقة SD أو بطاقة SD صغيرة أو وحدة eMMC بسعة 8 GB على الأقل.
- انسخ الصورة التي تم تنزيلها إلى جهاز التخزين باستخدام **dd**. هذا مشابه لعملية نسخ صورة ISO على مفتاح USB (انظر القسم ٤.١.٢. "نسخ الصورة على قرص DVD-ROM أو مفتاح USB").

```
dd if=kali-image.img of=/dev/something bs=512k
```

- قم بتوصيل بطاقة SD/eMMC بجهاز ARM الخاص بك.

❖ قم بتشغيل جهاز ARM وقم بتسجيل الدخول إليه (المستخدم "root"، كلمة المرور "toor") ||هذا قديما، أما الأن kali/kali||. إذا لم يكن لديك شاشة متصلة، فسيتعين عليك معرفة عنوان IP الذي تم تعيينه عبر DHCP والاتصال بهذا العنوان عبر SSH. تحتوي بعض خوادم DHCP على أدوات أو واجهات ويب لإظهار leases الحالية. إذا لم يكن لديك أي شيء من هذا القبيل، فاستخدم الشم (sniffer) للبحث عن حركة مرور DHCP lease.

❖ قم بتغيير كلمة المرور وقم بإنشاء مفاتيح مضيف SSH جديدة، خاصة إذا كان الجهاز سيتم تشغيله بشكل دائم على شبكة عامة! الخطوات بسيطة نسبيًا، راجع إنشاء مفاتيح مضيف SSH جديدة.

❖ استمتع بجهاز ARM الجديد الذي يعمل بنظام Kali Linux!

حالات خاصة ووثائق أكثر تفصيلاً

هذه الإرشادات عامة، وبينما تعمل مع معظم الأجهزة، هناك دائمًا استثناءات. على سبيل المثال، تتطلب أجهزة Chromebook وضع المطور وتتطلب الأجهزة الأخرى ضغطًا خاصًا على المفاتيح للإقلاع من الوسائط الخارجية.

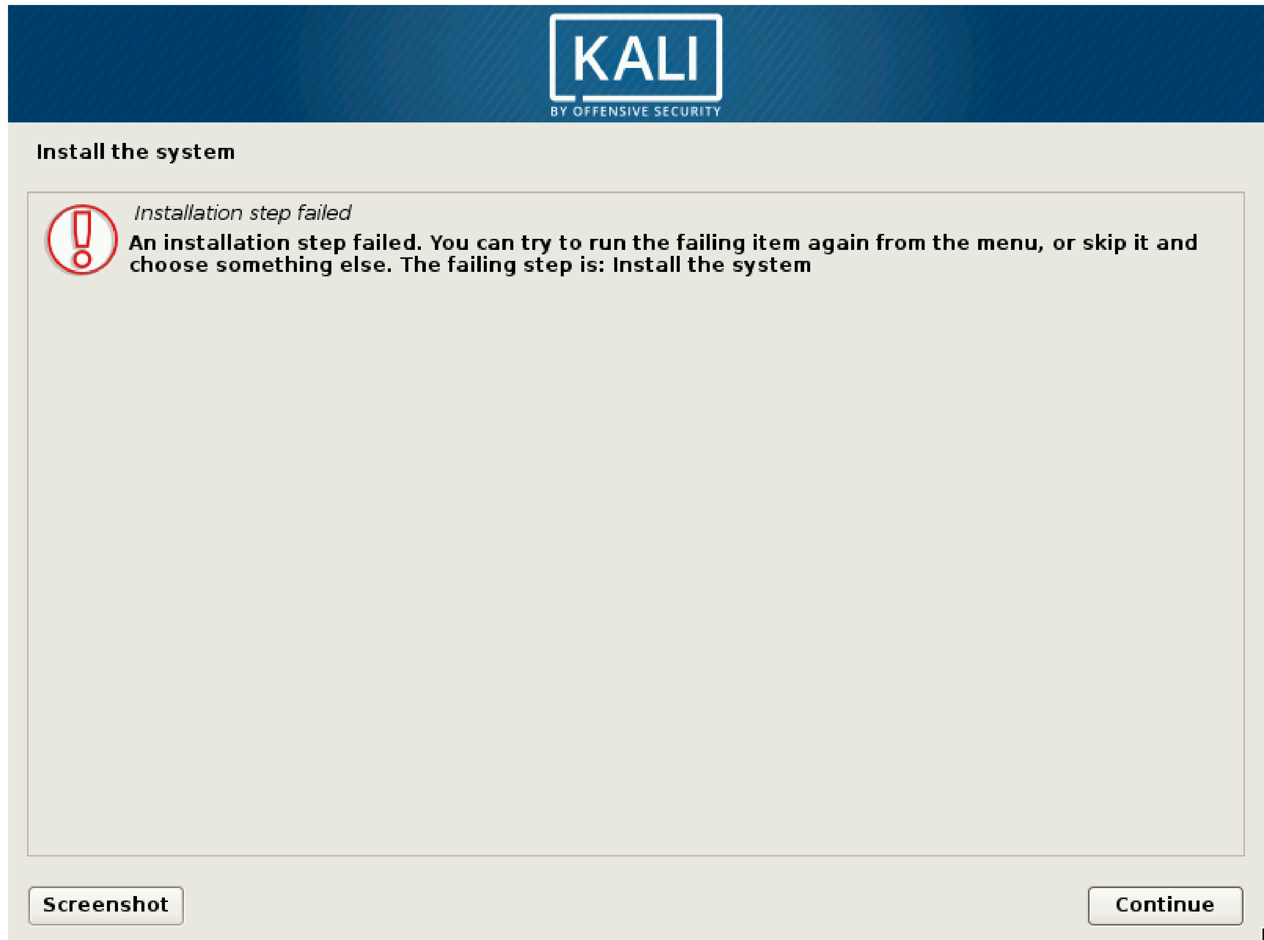
نظرًا لأن أجهزة ARM تُضاف بشكل متكرر نسبيًا ومواصفاتها حيوية للغاية، فلن نغطي تعليمات التثبيت المحددة لأجهزة ARM المختلفة هنا. بدلاً من ذلك، ارجع إلى قسم "Kali on ARM" المخصص في موقع وثائق Kali للحصول على معلومات حول كل أجهزة ARM المدعوم بواسطة Offensive Security:

http://docs.kali.org/category/kali-on-arm

٥.٤ استكشاف أخطاء التثبيت وإصلاحها

المثبت موثوق للغاية، ولكن قد تواجه أخطاء أو تواجه مشاكل خارجية مثل: مشاكل الشبكة، والمرايا السيئة، ومساحة القرص غير كافية. وبسبب هذا، من المفيد جدًا أن تكون قادرًا على استكشاف المشكلات التي تظهر في عملية التثبيت وإصلاحها.

عندما يفشل برنامج التثبيت، سيظهر لك شاشة غير مفيدة إلى حد ما مثل الشاشة الموضحة في الشكل ٢٦.٤ "فشل خطوة التثبيت".



شكل ٢٦.٤ "فشل خطوة التثبيت"

في هذه المرحلة، من الجيد أن تعرف أن المثبت يستخدم وحدات تحكم افتراضية متعددة: الشاشة الرئيسية التي تراها تعمل إما على وحدة التحكم الخامسة (للمثبت الرسومي، **CTRL + Alt + F5**) أو على وحدة التحكم الأولى (للمثبت النصي، **Shift + F4**). في كلتا الحالتين، تعرض وحدة التحكم الرابعة (**CTRL + Shift + F4**) سجلات لما يحدث ويمكنك عادةً رؤية رسالة خطأ أكثر فائدة هناك، مثل تلك الموجودة في الشكل ٢٧.٤. "شاشة السجل للمثبت"، والتي يكشف أن مساحة المثبت قد نفدت.

```
tion:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 88:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/choose_partition/60partition_tree/do_op
tion:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 88:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/free_space/50new/do_option:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 226:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/free_space/50new/do_option:
Apr 15 19:04:24 main-menu[833]: (process:5559): line 226:
Apr 15 19:04:24 main-menu[833]: (process:5559): /lib/partman/active_partition/copy/choices: not foun
d
Apr 15 19:04:24 main-menu[833]: (process:5559):
Apr 15 19:04:24 main-menu[833]: DEBUG: resolver (libgcc1): package doesn't exist (ignored)
Apr 15 19:04:24 main-menu[833]: INFO: Menu item 'live-installer' selected
Apr 15 19:04:24 base-installer: info: Using squashfs support for /cdrom/live/filesystem.squashfs
Apr 15 19:04:24 anna-install: Installing squashfs-modules
Apr 15 19:04:24 anna[8545]: DEBUG: resolver (kernel-image-4.3.0-kali1-amd64-di): package doesn't exi
st (ignored)
Apr 15 19:04:24 anna[8545]: DEBUG: retrieving squashfs-modules-4.3.0-kali1-amd64-di 4.3.3-5kali4
Apr 15 19:04:24 kernel: [  165.758382] squashfs: version 4.0 (2009/01/31) Phillip Lougher
Apr 15 19:04:24 kernel: [  165.764051] loop: module loaded
Apr 15 19:04:45 base-installer: error: The tar process copying the live system failed (only 9238 out
 of 119223 files have been copied, last file was ).
Apr 15 19:04:45 main-menu[833]: (process:8491): tar: write error: No space left on device
Apr 15 19:04:45 main-menu[833]: (process:8491): tar: write error: Broken pipe
Apr 15 19:04:45 main-menu[833]: WARNING **: Configuring 'live-installer' failed with error code 1
Apr 15 19:04:45 main-menu[833]: WARNING **: Menu item 'live-installer' failed.
_
```

شكل ٢٧.٤. "شاشة السجل للمثبت"

الكونسول الثاني والثالث (**CTRL + Shift + F2** و **CTRL + Shift + F3**، على التوالي) صدفات المضيف التي يمكنك استخدامها للتحقيق في الوضع الحالي بمزيد من التفاصيل. يتم توفير معظم أدوات سطر الأوامر بواسطة BusyBox لذا فإن مجموعة الميزات محدودة نوعًا ما، ولكنها كافية لمعرفة معظم المشاكل التي من المحتمل أن تواجهها.

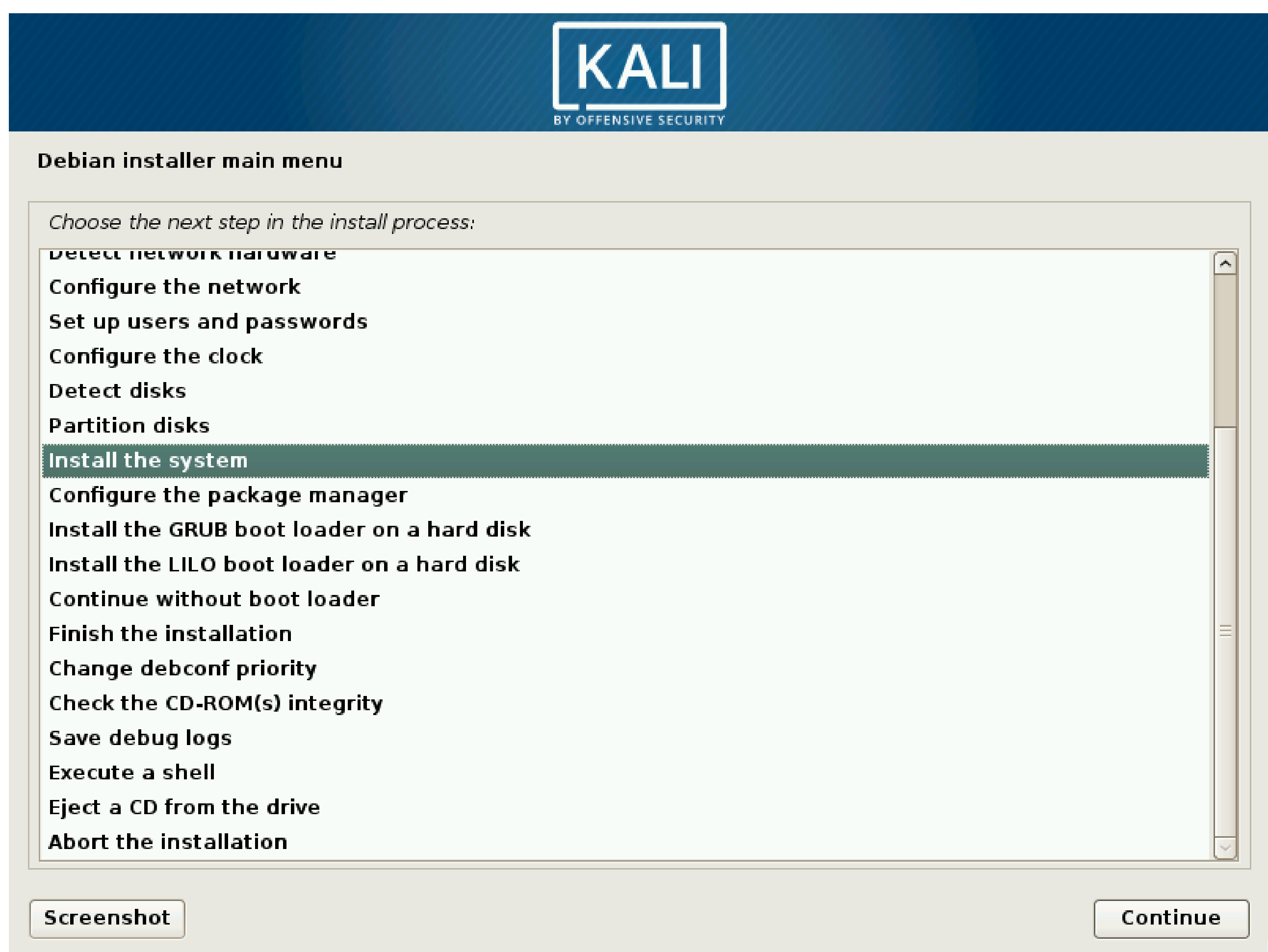
ما يمكن القيام به في صدفة المثبت

يمكنك فحص قاعدة بيانات debconf وتعديلها باستخدام `debconf-get` و `debconf-set`. تعتبر هذه الأوامر ملائمة بشكل خاص لاختبار قيم الـ preseeding.

يمكنك فحص أي ملف (مثل سجل التثبيت الكامل المتوفر في **/var/log/syslog**) بأمر **`cat`** أو **`more`**. يمكنك تعديل أي ملف باستخدام الأمر **`nano`**، بما في ذلك جميع الملفات المثبتة على النظام. سيتم وصل نظام الملفات الجذر بـ **/target** بمجرد اكتمال خطوة التقسيم لعملية التثبيت.

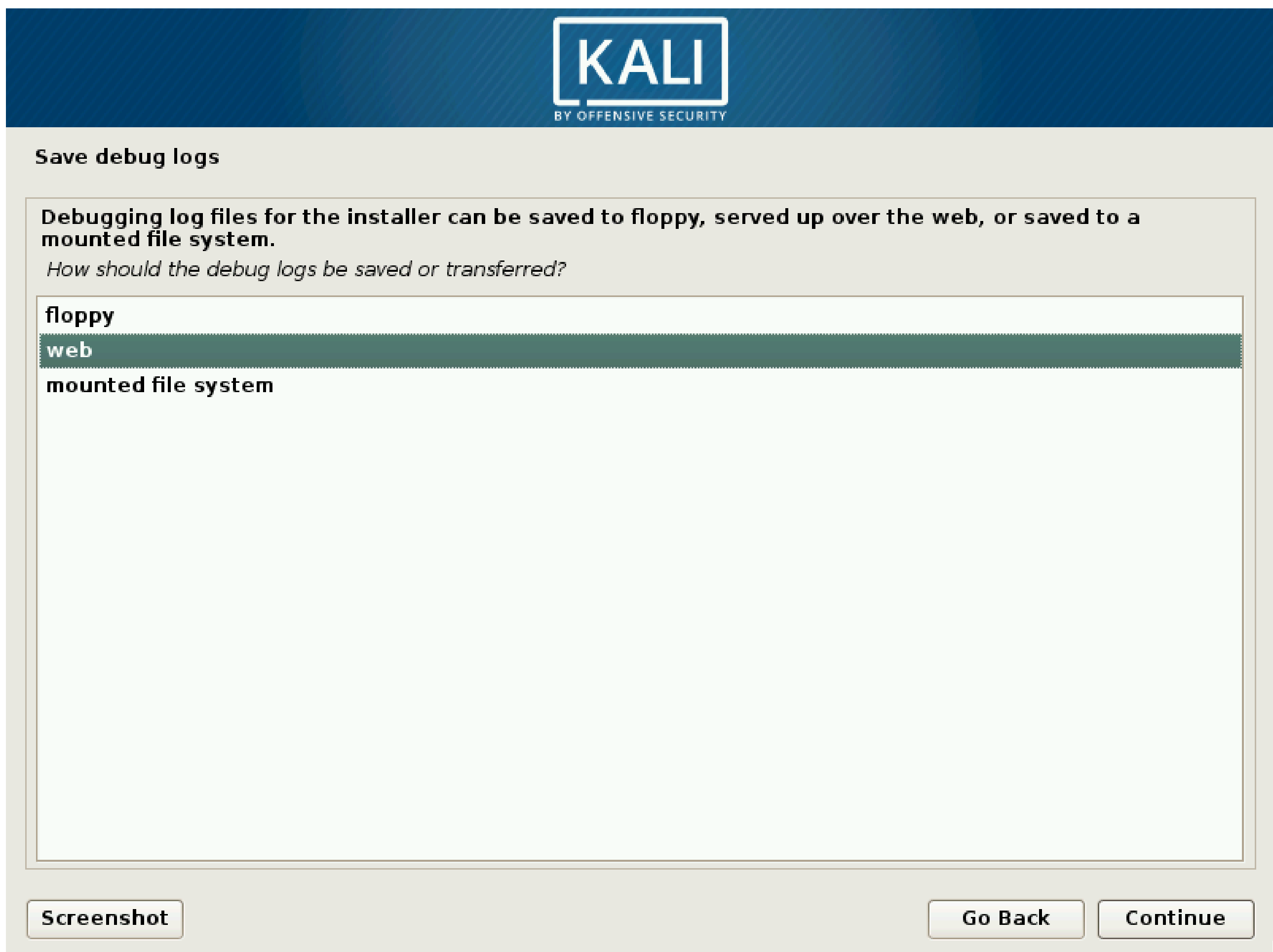
بمجرد تكوين الوصول إلى الشبكة، يمكنك استخدام **`wget`** و **`nc`** (netcat) لاسترداد البيانات وتصديرها عبر الشبكة.

بمجرد النقر فوق "**متابعة**" من شاشة فشل التثبيت الرئيسية (الشكل ٢٦.٤ "فشل خطوة التثبيت")، ستتم إعادتك إلى شاشة لن تراها عادةً (القائمة الرئيسية الموضحة في الشكل ٢٨.٤ "القائمة الرئيسية للمثبت")، مما يسمح لك بتشغيل خطوات التثبيت واحدة تلو الأخرى. إذا تمكنت من إصلاح المشكلة من خلال الوصول إلى الصدفة shell (تهانينا!)، فيمكنك إعادة محاولة الخطوة التي فشلت.



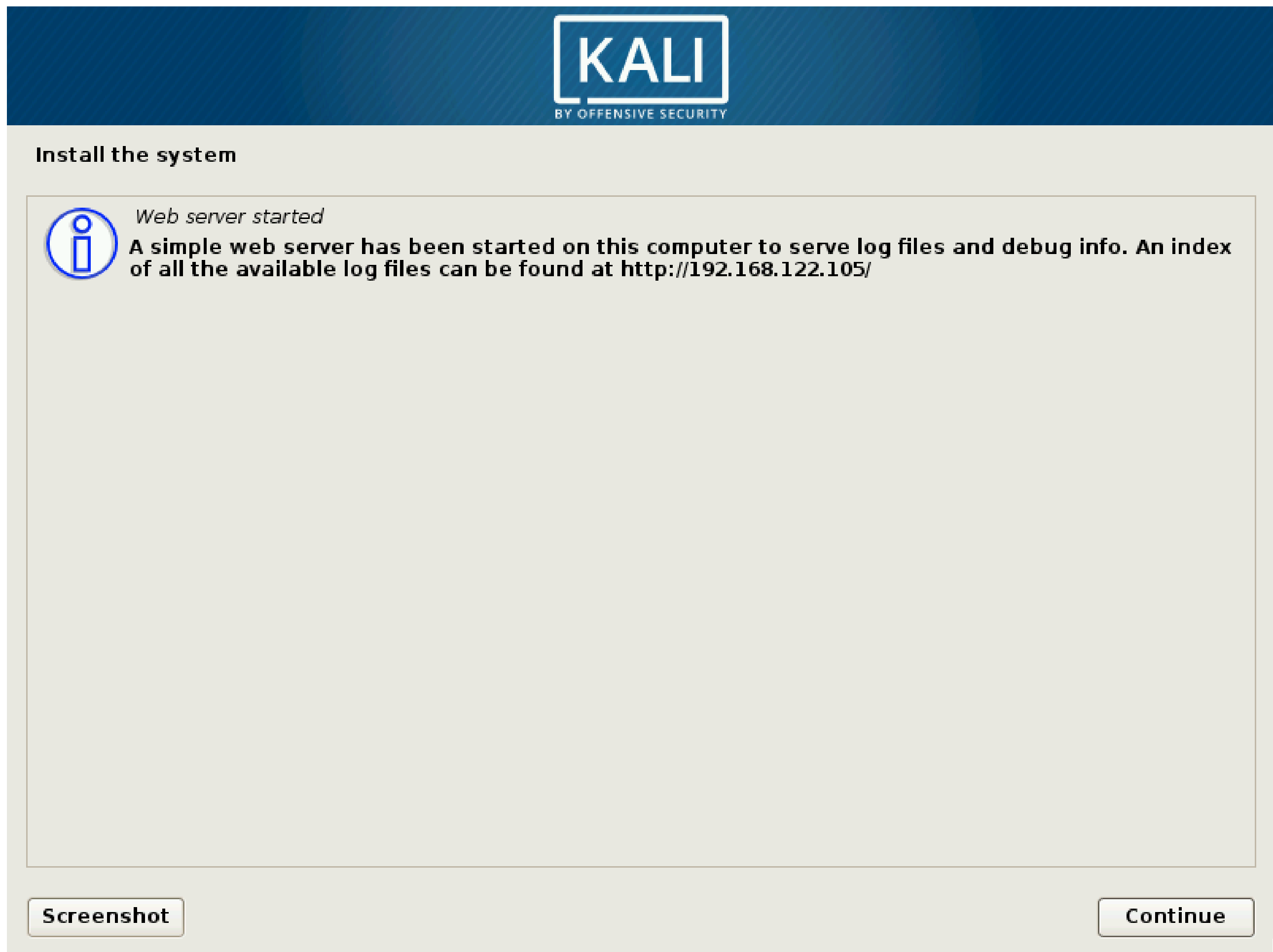
شكل ٢٨.٤ "القائمة الرئيسية للمثبت"

إذا كنت غير قادر على حل المشكلة، فقد تحتاج إلى تقديم تقرير خطأ. يجب أن يتضمن التقرير بعد ذلك سجلات المثبت، والتي يمكنك استردادها باستخدام وظيفة "حفظ سجلات تصحيح الأخطاء" "Save debug logs" في القائمة الرئيسية. يوفر طرقًا متعددة لتصدير السجلات، كما هو موضح في الشكل ٢٩.٤ "حفظ سجلات التصحيح (٢/١)".



شكل ٢٩.٤ "حفظ سجلات التصحيح (٢/١)

الطريقة الأكثر ملاءمة، والطريقة التي نوصي بها، هي السماح للمثبت ببدء خادم ويب يستضيف ملفات السجل (الشكل ٣٠.٤ "حفظ سجلات التصحيح (٢/٢)"). يمكنك بعد ذلك تشغيل متصفح من حاسوب آخر على نفس الشبكة وتنزيل جميع ملفات السجل ولقطات الشاشة التي التقطتها باستخدام زر **لقطة الشاشة "ScreenShot"** المتاح في كل شاشة.



شكل ٣٠.٤ "حفظ سجلات التصحيح (٢/٢) "

٦.٤. ملخص

في هذا الفصل، ركزنا على عملية تثبيت Kali Linux. ناقشنا الحد الأدنى من متطلبات التثبيت لـ Kali Linux، وعملية التثبيت لأنظمة الملفات القياسية والمشفرة بالكامل، والـ pre-seeding، والتي تسمح بالتثبيتات غير المراقبة "unattended"، وكيفية تثبيت Kali Linux على مختلف أجهزة ARM، وما الذي تفعله في حالات فشل التثبيت النادرة.

نصائح التلخيص:

❖ تختلف متطلبات التثبيت لـ Kali Linux من خادم SSH أساسي بدون سطح مكتب، مثل ذاكرة وصول عشوائي بسعة 128 MB (512 MB موصى بها) ومساحة قرص 2 GB، للـ:

higher-end kali-linux-full meta-package

❖ مع الحد الأدنى 2048 MB من ذاكرة الوصول العشوائي و 20 GB من مساحة القرص. بالإضافة إلى ذلك، يجب أن يحتوي جهازك على وحدة معالجة مركزية (CPU) مدعومة على الأقل ببنية amd64 أو i386 أو armel أو armhf أو arm64.

❖ يمكن تثبيت Kali بسهولة كنظام تشغيل أساسي، أو إلى جنب أنظمة تشغيل أخرى من خلال التقسيم وتعديل محمل الإقلاع، أو كنظام افتراضي.

❖ لضمان سرية بياناتك، يمكنك إعداد أقسام مشفرة. سيؤدي ذلك إلى حماية بياناتك في حالة فقدان أو سرقة الحاسوب المحمول أو محرك الأقراص الثابتة.

❖ يمكن أيضًا تشغيل المثبت تلقائيًا من خلال تصحيح debconf، وهي وظيفة تسمح لك بتقديم إجابات غير مراقبة على أسئلة التثبيت.

❖ ملف preseed هو ملف نصي عادي يحتوي على عدة أسطر كل سطر يكون إجابة سؤال Debconf واحد. يتم تقسيم السطر على أربعة حقول مفصولة بمسافة بيضاء (مسافات أو tabs). يمكنك الحصول على إجابات مسبقة للمثبت عن طريق معلمات الإقلاع، مع ملف preseed في البداية، أو ملف preseed على وسائط الإقلاع، أو مع ملف preseed من الشبكة.

❖ يعمل Kali Linux على مجموعة متنوعة من الأجهزة القائمة على ARM مثل أجهزة الحاسوب المحمولة وأجهزة الحاسوب المدمجة ولوحات المطور. تثبيت ARM واضح إلى حد ما. قم بتنزيل الصورة الصحيحة، وقم بنسخها على بطاقة SD، أو محرك أقراص USB، أو وحدة تحكم مدمجة للوسائط المتعددة (eMMC)، وقم بتوصيلها، وإقلاع جهاز ARM، والعثور على جهازك على الشبكة، وتسجيل الدخول، وتغيير كلمة مرور SSH ومفاتيح مضيف SSH.

❖ يمكنك تصحيح عمليات التثبيت الفاشلة باستخدام وحدات التحكم الافتراضية (يمكن الوصول إليها باستخدام CTRL + Shift ومفاتيح الوظائف)، وأوامر debconf-get و debconf-set، أو قراءة ملف سجل var/log/syslog/، أو عن طريق إرسال تقرير خطأ مع استرداد ملفات السجل بوظيفة "حفظ سجلات التصحيح" "Save debug logs" الخاصة بالمثبت.

الآن بعد أن ناقشنا أساسيات Linux وتثبيت Kali Linux، دعنا نناقش التكوين حتى تتمكن من البدء في تخصيص Kali لتناسب احتياجاتك.

التمرين الأول، للفصل الرابع - تثبيت مشفر القرص الكامل لـ Kali Linux

١. ما هو الحد الأدنى من الموارد المطلوبة لـ VM؟

٢. قم بتثبيت تشفير قياسي كامل افتراضي لـ Kali Linux على VM جديد. تأكد من أن الـ VM النهائي في وضع NAT.

٣. ما هي التقنيات المستخدمة للتشفير؟

الإجابات:

١. نأمل أنك لم تكن بحاجة إلى هذه الإجابة حقًا، وقد ألقيت نظرة خاطفة لأنك كنت فضوليًا. RAM 2 GB، 20 GB مساحة على القرص!

٢. تحقق من الفصل الرابع لإجراءات التثبيت. للتوضيح، الهدف هنا هو تثبيت Kali بنظام الملفات المشفر على VM جديد عن طريق الإقلاع من ISO والمتابعة يدويًا خلال التثبيت. الهدف ليس تشغيل ملف vmx. الموفر من Kali.

٣. LUKS وLogical Volume Management (LVM).

التمرين الثاني، للفصل الرابع - التثبيت غير المراقب لـ Kali Linux

١. إنشاء VM جديد، بالحد الأدنى من المتطلبات.

٢. أكمل التثبيت القياسي، الافتراضي، باستخدام ملف preseed - مستضاف عبر HTTP (أو HTTPS). ملفك المضغوط هو:

https://www.kali.org/dojo/preseed.cfg .

٣. تأكد من أن التثبيت غير مراقب تمامًا: يجب عليك تحديد اللغة وخريطة لوحة المفاتيح واسم المضيف والمجال.

الإجابات:

١. الحد الأدنى من المتطلبات: GB 2 من ذاكرة الوصول العشوائي، مساحة القرص 20 GB. أنت تعرف هذا الآن، أليس كذلك؟

٢. هذا إلى حد كبير تثبيت قياسي عن طريق معلمات الإقلاع المعدلة. فيما يلي معلمات إقلاع مقترحة:

```
preseed/url=https://www.kali.org/dojo/preseed.cfg
locale=en_US keymap=us hostname=kali domain=local.
lan
```

لاحظ أن معلمات locale وkeymap وhostname وdomain توضع على سطر أوامر النواة!

```
GNU GRUB  version 2.02~beta3-5

setparams 'Start installer'

        linux        /install/gtk/vmlinuz video=vesa:ywrap,mtrr vga=788 preseed/url\
=https://www.kali.org/dojo/preseed.cfg locale=en_US keymap=us hostname=kalima domai\
n=local.lan_
        initrd        /install/gtk/initrd.gz
```

سؤال زن: "لماذا لا يمكن لـ preseed اليدوي أن يتعامل مع معلمات اللغة وخريطة المفاتيح واسم المضيف والمجال؟"

سؤال جيد. تعتمد معلمات Preseeding على الطريقة المتنبأ بها. إذا كنت تستخدم ملفًا تم تقديره في الحرف الأول، فيمكنك عندئذٍ توقع جميع المعلمات حتى تلك التي كانت في وقت مبكر جدًا من العملية. إذا كنت تستخدم ملفًا preseed من الشبكة أو من صورة ISO نفسها، فسيتم تطبيق المتوقع بعد ذلك بقليل في عملية التثبيت ويلزم توقع المعلمات المبكرة في سطر أوامر النواة.

وبدلاً من ذلك، يمكنك أيضًا استخدام المعلمات auto=true و`priority=critical`.

```
preseed/url=https://www.kali.org/dojo/preseed.cfg
auto=true priority=critical
```

إذا لم تكن تعرف هذا، صعد لعبتك! انتبه! تم ذكر معلمات الإقلاع التلقائي والأولويات بشكل خاص في الفصل ٣.٤. لا تعتقد أنه يمكنك تخطي كل المواد وتمريرها. نحن نراقبك.

التمرين الثالث، الفصل الرابع - تثبيت ARM القياسي لـ Kali Linux

إذا كان لديك Raspberry Pi أو جهاز مشابه، فاخذ نسخة من صورة ARM المناسبة من هنا (https://www.offensive-security.com/kali-linux-arm-images/). انسخه على بطاقة SD وجربه.

الإجابة:

هناك مشكلة الدجاج والبيض هنا. للحفاظ على توحيد الأمور، نفضل أن تقوم بتنفيذ كل هذه الخطوات في كالي. بهذه الطريقة، لديك كل الأدوات التي تحتاجها، ويمكننا إرشادك من خلالها دون شرح العملية على أنظمة تشغيل متعددة (Windows وOS X وLinux). ولكن من أجل القيام بذلك من كالي، نحتاج إلى نقل الصورة إلى كالي والطريقة الأكثر موثوقية ومباشرة للقيام بذلك هي بـ **scp** الذي يعتمد على خدمة **ssh**. لكننا لن نتطرق لـ SSH حتى الفصل التالي.

لذا، على الرغم من أنها ليست مثالية، إلا أننا سنغض الطرف عن إجراء SSH هنا حتى نتمكن من المضي قدمًا وسنناقش تفاصيل أكثر في الفصل التالي. عن تركيب كالي الخاص بك:

قم بتحرير الملف /etc/ssh/sshd_config. ابحث عن سطر `PermitRootLogin without-password` وقم بتغييره لـ `PermitrootLogin yes`.

بدء sshd:

```
root@kali:~# systemctl start ssh
```

تمكين sshd عند الإقلاع:

```
root@kali:~# systemctl enable ssh
```

الآن، يجب أن تكون قادر على الوصول لـ ssh في جهازك كـ root/toor:

```
Host Machine:~ j$ ssh root@192.168.1.12
root@192.168.1.12's password :
The programs included with the Kali GNU/Linux system are free software؛
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar  1 21:43:37 2017 from 192.168.1.71
```

الآن يمكننا نقل ملف xz إلى Kali VM. حاول تجنب السحب والإسقاط VM. يمكن أن يسبب مشكلة:

```
scp kali-2017.01-rpi2.img.xz root@192.168.60.185:/root
```

بعد ذلك، ادخل بطاقة SD (بحد أدنى 8 GB) وابحث عن معرف القرص المناسب:

```
root@kali:~# dmesg
[194628.402969] sd 3:0:0:0: Attached scsi generic sg2 type 0
[194628.410035] sd 3:0:0:0: [sdb] 15564800 512-byte logical blocks: (7.97 GB/7.42 GiB)
[194628.410821] sd 3:0:0:0: [sdb] Write Protect is off
[194628.410823] sd 3:0:0:0: [sdb] Mode Sense: 03 00 00 00
[194628.411936] sd 3:0:0:0: [sdb] No Caching mode page found
```

```
[194628.411940] sd 3:0:0:0: [sdb] Assuming drive cache: write through
[194628.420751] sdb: sdb1
```

فك ضغط ملف xz:

```
root@kali:~# cd /root
root@kali:~# unxz kali-2017.01-rpi2.img.xz
```

(بدلاً من ذلك، تحقق من xzcat).

قم بتشغيل أمر **dd** باستخدام معرف القرص الصحيح (dev/sdb/ في حالتنا). تحذير! لا تقم بنسخ هذه القيم ببساطة فقط! بل قم بتغييرها إلى مسار محرك الأقراص الصحيح المطابق لبطاقة SD الخاصة بك.

```
root@kali:~# dd if=/root/kali-2017.01-rpi2.img of=/dev/sdb bs=1M
7000+0 records in
7000+0 records out
7340032000 bytes (7.3 GB, 6.8 GiB) copied, 1356.87 s, 5.4 MB/s
```

ادخل SD الخاصة بك واقلع من Kali Pi الجديد. ستحتاج إلى توصيل HDMI لمعرفة ما يحدث ولوحة مفاتيح USB وفأرة للكتابة والنقر. أي يجب عليك توصيل كابل إيثرنت للحصول على الشبكة (إنه DHCP). أوه، ولا يوجد استماع SSH افتراضياً. ألا تمنى لو كان لديك المزيد من السيطرة على الأشياء؟ إذن واصل القراءة.

استكشاف Zen-التمرين الرابع، للفصل الرابع - تثبيت KAL Linux ARM المخصص

في التمرين السابق، قمنا بإجراء تثبيت ARM قياسي. كما رأيتم، كانت النتائج أقل من مثيرة. على الرغم من أننا لا نغطي هذا في الكتاب، نعتقد أنه من المهم أن ترى كيفية إنشاء صورة مخصصة. يمكنك ممارسة هذا التمرين على أي جهاز ARM مدعوم، ولكننا سنستخدم Raspberry Pi3. تحقق من قائمة أجهزة ARM المدعومة. سننشئ صورة Kali ARM مخصصة تحتوي على:

- ❖ الحد الأدنى من الحزم.
- ❖ بدون بيئة سطح المكتب (بلا رأس).
- ❖ عنوان IP ثابت على eth0 لذلك لا يتعين علينا البحث عن Pi
- ❖ أدوات مثل `ifconfig` مثبتة.
- ❖ تبدأ خدمة SSH مع الإقلاع، مع تثبيت مفتاح SSH العام مسبقًا.

انطلق، انظر للإجابة. هذا استكشاف، على كل حال.

الإجابة:

قم بتنزيل وتثبيت البرامج النصية للبناء "build scripts"، و build dependencies، و cross compiler.

```
mkdir /root/arm-stuff
cd /root/arm-stuff
```

بعد ذلك، نحتاج لـ cross-compiler لـ armhf. تحتوي هذه الحزمة على إصدارات تم إنشاؤها مسبقًا من Linaro GCC و Linaro GDB ، وهو gdbserver (برنامج يسمح لك بتشغيل GDB على جهاز مختلف عن الجهاز الذي يقوم بتشغيل البرنامج الذي يتم تصحيحه)، وجذر النظام (بجميع الرؤوس و المكتبات لربط البرامج) والتعليمات التي في share/doc:

```
git clone https://gitlab.com/kalilinux/packages/gcc-arm-linux-gnueabihf-4-7
```

سيحتاج كالي للملفات الموجودة في bin/ من أجل للبناء:

```
export PATH=${PATH}:/root/arm-stuff/gcc-arm-linux-gnueabihf-4.7/bin
```

بعد ذلك، السحر الحقيقي. سنأخذ نصوص بناء كالي لينكس ARM، ونستخدمها لإنشاء صورنا الرسمية لـ Kali Linux ARM على http://www.kali.org/downloads.

```
git clone https://gitlab.com/kalilinux/build-scripts/kali-arm
cd ~/arm-stuff/kali-arm-build-scripts
```

بعد ذلك، قم بتثبيت dependencies المطلوبة. هذا سوف يستغرق بضع دقائق:

```
./build-deps.sh
```

بعد ذلك، قم بتحرير البرنامج النصي لبناء ARM، وقم بتغيير الحقول المطلوبة. نقوم بتحرير نص Raspberry Pi3 Kali ARM. يحتوي على nexmon مضمن: إطار تصحيح البرامج الثابتة المستند إلى C لشرائح WiFi من Broadcom/Cypress التي تتيح وضع المراقبة وحقن الإطار والمزيد.

في حالتنا يمكننا إزالة **سطح المكتب**، ومعظم **الأدوات والإضافات**. بالإضافة إلى ذلك، نريد إعداد عنوان Raspberry Pi IP ليكون IP ثابتًا حتى نتمكن من SSH إليه لاحقًا. بالطبع، يجب أن يبدأ SSH في وقت الإقلاع، ولديه مفتاحنا العام.

```
nano rpi3-nexmon.sh
```

أولاً، سنقوم بالتعليق على أقسام **سطح المكتب والإضافات**، وإجراء تغييرات على أقسام **الأدوات والخدمات**:

```
#desktop="fonts-croscore fonts-crosextra-caladea fonts-crosextra-carlito gnome-theme-kali gtk3-engines-xfce kali-desktop-xfce kali-root-login lightdm network-manager network-manager-gnome xfce4 xserver-xorg-video-fbdev xserver-xorg-input-evdev xserver-xorg-input-synaptics"

#tools="aircrack-ng ethtool hydra john libnfc-bin mfoc nmap passing-the-hash sqlmap usbutils winexe wireshark net-tools"

tools="aircrack-ng nmap hostapd"


#services="apache2 openssh-server gnupg"

services="openssh-server gnupg"


#extras="iceweasel xfce4-terminal wpasupplicant python-smbus i2c-tools python-requests python-configobj python-pip"
```

سنقوم أيضًا بإجراء تغييرات على قسم **الحزم**، مع إزالة **سطح المكتب والإضافات**:

```
#packages="${arm} ${base} ${desktop} ${tools}
${services} ${extras}"
packages="${arm} ${base} ${tools} ${services}"
```

أبعد من ذلك، سنقوم بإخراج eth0 من dhcp وتعيين عنوان ثابت:

```
auto eth0
        iface eth0 inet static
        address 192.168.1.12
        netmask 255.255.255.0
        gateway 192.168.1.1
EOF
```

يمكن عرض التغييرات التي أجريناها بطريقة أخرى باستخدام أداة **diff**، التي تقارن الملفات. هنا نرى قبل وبعد. تُظهر الخطوط البيضاء الأسطر التي تتطابق بين الملفات (ولكن تم نقلها في هذه الحالة لأننا أدرجنا بعض الأسطر). تعرض الخطوط الحمراء عمليات الحذف، وتظهر الخطوط الخضراء الإضافات. لاحظ أنه في هذا الاختلاف، قمنا بحذف خطوط التكوين بدلاً من التعليق عليها:

```
root@kali:~/arm-stuff/kali-arm-build-scripts# git diff
diff --git a/rpi3-nexmon-bh.sh b/rpi3-nexmon-bh.sh
index 0afe723..4676e21 100755
--- a/rpi3-nexmon-bh.sh
+++ b/rpi3-nexmon-bh.sh
@@ -25,14 +25,12 @@ TOPDIR=`pwd`

 arm="abootimg cgpt fake-hwclock ntpdate u-boot-tools vboot-utils vboot-kernel-utils"
 base="e2fsprogs initramfs-tools kali-defaults kali-menu parted sudo usbutils"
-desktop="fonts-croscore fonts-crosextra-caladea fonts-crosextra-carlito gnome-theme-kali gtk
work-manager network-manager-gnome xfce4 xserver-xorg-video-fbdev xserver-xorg-input-evdev xs
-tools="aircrack-ng ethtool hydra john libnfc-bin mfoc nmap passing-the-hash sqlmap usbutils
-services="apache2 openssh-server"
-extras="iceweasel xfce4-terminal wpasupplicant python-smbus i2c-tools python-requests python
+tools="aircrack-ng nmap hostapd"
+services="openssh-server"
 # kernel sauces take up space yo.
 size=7000 # Size of image in megabytes

-packages="${arm} ${base} ${desktop} ${tools} ${services} ${extras}"
+packages="${arm} ${base} ${tools} ${services}"
 architecture="armhf"
 # If you have your own preferred mirrors, set them here.
 # After generating the rootfs, we set the sources.list to the default settings.
@@ -73,7 +71,10 @@ auto lo
 iface lo inet loopback

 auto eth0
-iface eth0 inet dhcp
+       iface eth0 inet static
+       address 192.168.1.12
+       netmask 255.255.255.0
+       gateway 192.168.1.1
 EOF
```

بمجرد إجراء التغييرات، يمكننا تشغيل البرنامج النصي للبناء بمعرف أنيق (1.0 "a lame" في هذا المثال). لاحظ أن هذا قد يستغرق أكثر من ساعة، بناءً على وحدة المعالجة المركزية والذاكرة والنطاق الترددي:

```
./rpi3-nexmon.sh 1.0
```

بمجرد الانتهاء من ذلك، يجب أن يكون لديك ثلاثة ملفات:

```
root@kali:~/arm-stuff/kali-arm-build-scripts# ls -l
rpi3-nexmon-bh-1.0/
total 553496
-rw-r--r-- 1 root root        91 Aug  5 12:14 kali-
1.0-rpi3-nexmon.img.sha256sum
-rw-r--r-- 1 root root 566765348 Aug  5 12:23 kali-
1.0-rpi3-nexmon.img.xz
-rw-r--r-- 1 root root        94 Aug  5 12:23 kali-
1.0-rpi3-nexmon.img.xz.sha256sum
```

الآن، يمكنك حرق ISO إلى SD لاختبار الصورة. كما هو الحال دائمًا، تأكد من تحديد معرف الجهاز الصحيح. في حالتنا، dev/sdb/. يمكن أن يستغرق ذلك 20 دقيقة أو أكثر، عند تشغيله من جهاز افتراضي تم تكوينه بشكل صحيح:

```
root@kali:~# cd /root/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0/

root@kali:~/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0# ls

kali-1.0-rpi3-nexmon.img.sha256sum  kali-1.0-rpi3-nexmon.img.xz  kali-1.0-rpi3-nexmon.img.xz.sha256sum

root@kali:~/arm-stuff/kali-arm-build-scripts/rpi3-nexmon-bh-1.0# xzcat kali-1.0-rpi3-nexmon.img.xz | dd of=/dev/sdb bs=1M
```

بعد ذلك، قم بتشغيل Kali Pi. يجب أن تجده على 192.168.1.12، ويجب أن يكون ssh مفتوحًا. أوه، ومكافأة! **ifconfig** يعمل!

استكشاف Zen - التمرين الخامس ، للفصل الرابع - كالي لينكس ARM chroot

إذا كان البناء الذي صنعته لم يكن مناسبا. لحسن الحظ أنه يمكنك تغييره. في هذا المثال، لنفترض أنك نسيت تثبيت بعض الحزم، مثل net-tools و dnsmasq و mlocate. بدلاً من إعادة تثبيت الجهاز وإعادة تصويره، قم بالتبديل إلى بطاقة RPi3 SD من جهاز Kali الخاص بك وقم بإجراء التغييرات المطلوبة.

نظراً لأن هذا هو دليل تفصيلي، ولم يتم تناوله في الكتاب، فاستمر وانظر للإجابة واكتشف.

الإجابة:

ستبدأ ببطاقة SD من تمرين سابق. في هذا المثال، نستخدم الصورة من التمرين السابق (التمرين الرابع) - بناءنا المخصص. أولاً، قم بتثبيت أدوات الترجمة بواسطة **qemu** والأدوات ذات الصلة في كالي:

```
apt-get install qemu qemu-user qemu-user-static
```

دعنا نقوم بإنشاء مجلد mnt/sd/ للحفاظ على المجلدات التي نعمل عليها منظمة:

```
mkdir /mnt/sd
```

احصل على تعيين محرك الأقراص dev/sd/ بإدخال بطاقة SD الخاصة بـ Pi (هي dev/sdc/). محول USB-SD الخاص بك يحدث فرقا. سنلتقط جميع حوامل محرك الأقراص الفعلية في لقطة واحدة.

```
root@kali:~# mount /dev/sdc2 /mnt/sd/
root@kali:~# ls -l /mnt/sd
total 88
drwxr-xr-x  2 root root  4096 Aug  5 11:36 bin
drwxr-xr-x  2 root root  4096 Jul 18 03:08 boot
drwxr-xr-x  4 root root  4096 Aug  5 11:15 dev
drwxr-xr-x 71 root root  4096 Mar  1 16:43 etc
drwxr-xr-x  2 root root  4096 Jul 18 03:08 home
drwxr-xr-x 13 root root  4096 Aug  5 12:11 lib
drwx------  2 root root 16384 Aug  5 11:39 lost+found
drwxr-xr-x  2 root root  4096 Aug  5 11:15 media
drwxr-xr-x  2 root root  4096 Aug  5 11:15 mnt
drwxr-xr-x  2 root root  4096 Aug  5 11:15 opt
drwxr-xr-x  2 root root  4096 Jul 18 03:08 proc
```

```
drwx------  2 root root  4096 Mar  1 16:43 root
drwxr-xr-x  4 root root  4096 Aug  5 11:15 run
drwxr-xr-x  2 root root  4096 Aug  5 11:36 sbin
drwxr-xr-x  2 root root  4096 Aug  5 11:15 srv
drwxr-xr-x  2 root root  4096 Jul 18 03:08 sys
drwxrwxrwt  7 root root  4096 Mar  1 18:40 tmp
drwxr-xr-x 10 root root  4096 Aug  5 11:15 usr
drwxr-xr-x 11 root root  4096 Aug  5 11:15 var
```

هل لاحظت كيف يتم الآن تعيين جميع مجلدات بطاقة SD الخاصة بـ Raspberry Pi على نظامك في /mnt/sd؟

قم بتحميل جميع "أنظمة الملفات الخاصة" في /mnt/sd. لاحظ أننا سنلغي خيارات التثبيت من /etc/fstab على بعض الخرائط التي تم تعيينها بالفعل مع الخيار **o**-:

```
mount -t proc none /mnt/sd/proc
mount -t sysfs none /mnt/sd/sys
mount -o bind /dev /mnt/sd/dev
mount -o bind /dev/pts /mnt/sd/dev/pts
```

دعونا نسحب أدوات تجميع emu. نحتاج إليها لتجميع عناصر ARM لأن هدفنا هو ARM!

```
cp /usr/bin/qemu-arm-static /mnt/sd/usr/bin
```

حان الوقت للدخول chroot! بمجرد الدخول إلى chroot، ستفترض جميع الإشادات التي ننفذها أن mnt/sd/ هو نظام ملفات الجذر الخاص بنا. إنها خدعة رائعة. لاحظ أننا قمنا بتعيين LAN=C لمنع التحذيرات المحلية في chroot الخاص بك:

```
LANG=C chroot /mnt/sd/
```

دعونا نجري بعض التغييرات على نظام ملفات Pi. هذا هو الجزء الرائع. كل هذا يحدث على نظام ملفات Pi الخاص بك!

```
# apt-get update
# apt-get install mlocate
# apt-get install net-tools
# apt-get install hostapd dnsmasq
```

تابع التكوين حسب الضرورة. بمجرد الانتهاء، اخرج من chroot وقم بإلغاء تحميل بطاقة SD.

```
root@kali:~# exit
```

نحتاج إلى إلغاء وصل كل المجلدات التي قمنا بوصلها (أو تثبيتها):

```
umount /mnt/sd/dev/pts
umount /mnt/sd/dev/
umount /mnt/sd/sys
umount /mnt/sd/proc
umount /mnt/sd
```

أخيرًا، أدخل بطاقة SD في Pi، وابدأ!

اختبار KLCP للفصل الرابع

١. ما هو التكوين الموصى به لخادم Kali SSH البسيط القائم على Intel بدون سطح مكتب (بلا رأس)؟

- 4096 MB RAM / 40 GB hard drive free space / i386 CPU
- 128 MB RAM / 1 GB hard drive free space / arm64 CPU
- 512 MB RAM / 2 GB hard drive free space / amd64 CPU
- 2048 MB RAM / 20 GB hard drive free space / SPARC CPU

٢. بشكل عام، أي من هذه ليست متطلبات الحد الأدنى لسطح المكتب كالي لينكس؟

- 4096 MB RAM / 40 GB hard drive free space
- 128 MB RAM / 1 GB hard drive free space
- 512 MB RAM / 2 GB hard drive free space
- 2048 MB RAM / 20 GB hard drive free space

٣. صح أو خطأ: سيفشل تثبيت Kali Linux إذا لم تختار مرآة للشبكة.

- صح
- خطأ

٤. صح أو خطأ: عند الإقلاع من mini.iso، سيفشل تثبيت Kali Linux إذا تعذر الكشف عن أجهزة الشبكة.

- صح
- خطأ

٥. ما هو نظام التقسيم الذي من المرجح أن يتأثر بخطأ المستخدم؟

- Guided – use entire Disk
- Guided – use entire disk and set up LVM
- Manual
- Guided – use entire disk and set up encrypted LVM

٦. ما هي طريقة التقسيم المفضلة للخوادم والأنظمة متعددة المستخدمين؟

- Separate /home, /var, and /tmp partitions
- Separate /home/ partition
- All files in one partition
- No Partitions

٧. سيؤدي تثبيت إصدار حديث من Windows بعد تثبيت Kali إلى:

- فشل بسبب تثبيت محمل الإقلاع السابق
- مسح محمل الإقلاع ومنع كالي من الإقلاع
- مسح كالي لينكس
- إنشاء إقلاع آمن للفشل لنظام كالي

٨. ما هو الغرض من preseed.cfg؟

- تعيين seed عشوائي لوظائف التشفير
- إنشاء افتراضيات معقولة لمعظم إعدادات المستخدم
- ملف التكوين الخاص بالبرنامج الخفي
- توفير إجابات محددة مسبقًا لأسئلة التثبيت

٩. ما هو الإجراء الأبسط والأكثر فعالية لتثبيت كالي على جهاز ARM؟

- استخدم الإنشاء المباشر "live-build" لإنشاء ملف ISO يستند على ARM
- استخدم mini.iso لإنشاء نظام أساسي، ثم قم بتشغيل `apt-get update`
- الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها واتبع خطوات التثبيت
- الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها وتسجيل الدخول باستخدام root/toor

١٠. ما الطريقة التي لا تتوفر بسهولة لحفظ سجلات تصحيح الأخطاء أثناء التثبيت الفاشل؟

- التخزين على القرص المرن
- حفظ السجلات على kali bug tracker
- عرض السجلات من خادم ويب
- حفظ السجلات لنظام ملفات موصول

الإجابات:

1. 512 MB RAM / 2 GB hard drive free space / amd64 CPU
2. 512 MB RAM / 2 GB hard drive free space

٣. خطأ

٤. صح

5. Manual
6. Separate /home, /var, and /tmp partitions

٧. مسح محمل الإقلاع ومنع كالي من الإقلاع

٨. توفير إجابات محددة مسبقًا لأسئلة التثبيت

٩. الإقلاع من صورة Kali ARM الرسمية التي تم التحقق منها وتسجيل الدخول باستخدام root/toor

١٠. حفظ السجلات على kali bug tracker

---((الفصل الخامس))---

في هذا الفصل، سنلقي نظرة على طرق مختلفة يمكنك من خلالها تكوين Kali Linux.

أولاً، في القسم 1.5، "تكوين الشبكة"، سنوضح لك كيفية تكوين إعدادات الشبكة باستخدام البيئة الرسومية وبيئة سطر الأوامر.

في القسم 2.5 "إدارة مستخدمي Unix ومجموعات Unix"، سنتكلم عن المستخدمين والمجموعات، ونوضح لك كيفية إنشاء وتعديل حسابات المستخدمين، وتعيين كلمات المرور، وتعطيل الحسابات، وإدارة المجموعات.

أخيرًا، سنناقش الخدمات في القسم 3.5، "تكوين الخوادم" وسنشرح كيفية إعداد الخدمات العامة والمحافظة عليها، ونركز أيضًا على الثلاث الخدمات المهمة للغاية وهي : SSH و PostgreSQL و Apache.

الإختصارا الواردة في هذا الفصل:

(SSH: **S**ecure **Sh**ell**)**, **(Gnome**: **G**NU **N**etwork **O**bject **M**odel **E**nvironment**)**

(GNU: **G**nu **N**ot **U**nix**)**, **(**Unix: ليس اختصارا**)**, **(IP**: **I**nternet **P**rotocol**)**

(Dhcp: **D**ynamic **H**ost **C**onfiguration **P**rotocol**)**

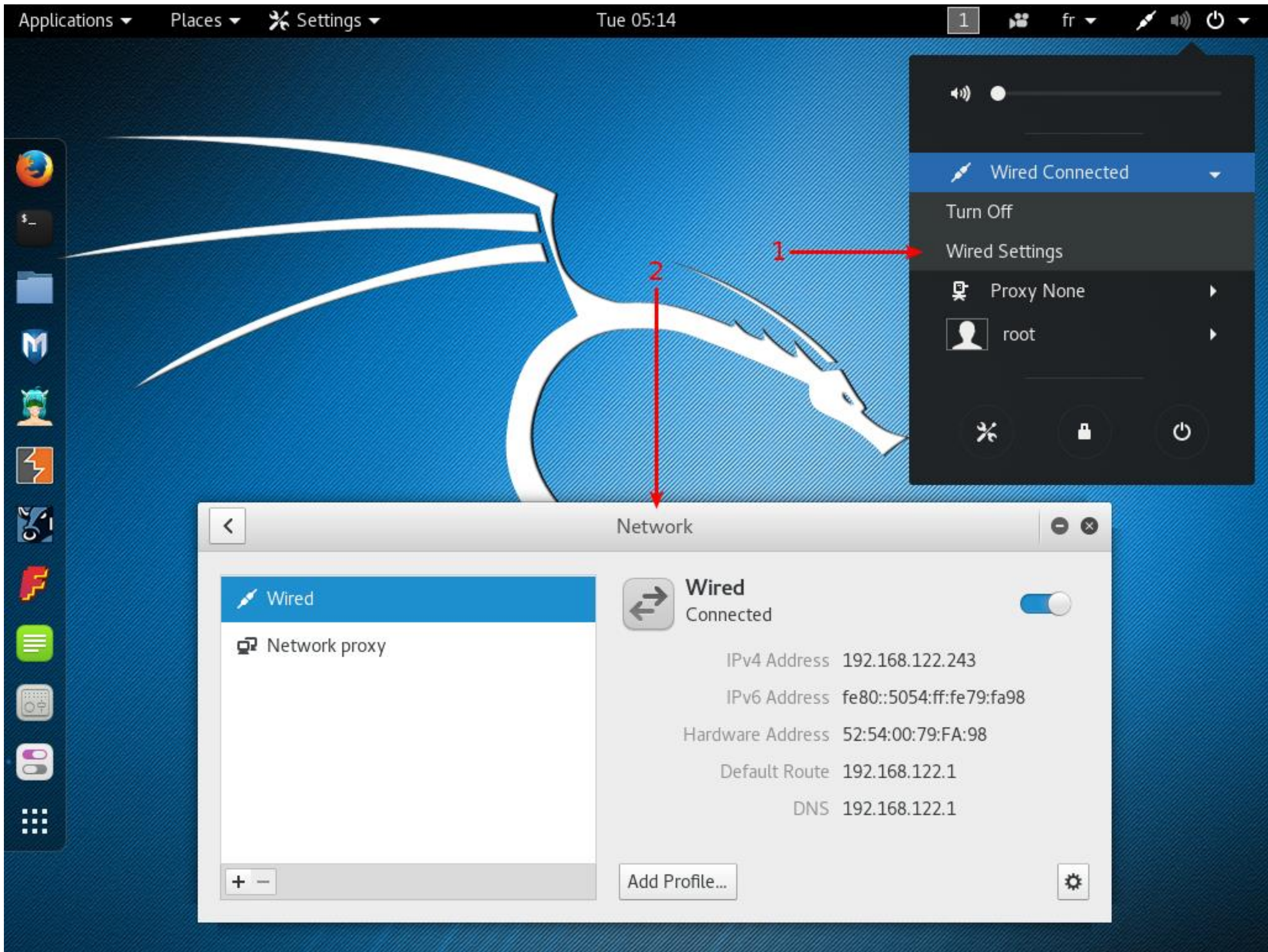
(MAC: **M**edia **A**ccess **C**ontrol**)**, **(SSID: S**ervice **S**et **ID**entifier**)**

(DNS: **D**omain **N**ame **S**ystem**)**, **(PPTP: P**oint-to-**P**oint **T**unneling **P**rotocol**)**.

1.5. تكوين الشبكة

١.١.٥. على سطح المكتب مع NetworkManager

في التثبيت العادي لسطح المكتب، سيكون لديك مدير شبكة –NetworkManager- مثبتاً بالفعل ويمكن التحكم فيه وتكوينه من خلال مركز التحكم في GNOME ومن خلال القائمة العلوية اليمنى كما هو موضح في الشكل .1.5. "شاشة تكوين الشبكة".



في شكل .1.5. "شاشة تكوين الشبكة".

يعتمد التكوين الافتراضي للشبكة على DHCP للحصول على عنوان IP وخادم DNS والبوابة، ولكن يمكنك استخدام رمز الترس في الزاوية اليمنى السفلية لتغيير التكوين بعدة طرق (على سبيل المثال: تعيين عنوان MAC والتبديل إلى إعداد static، قم بتمكين أو تعطيل IPv6، وإضافة

موجهات "رواتر"). يمكنك إنشاء ملفات تعريف لحفظ تكوينات شبكة سلكية متعددة والتبديل بينها بسهولة. بالنسبة للشبكات اللاسلكية، ترتبط إعداداتها تلقائيًا بمعرفها العام (SSID).

يعالج NetworkManager أيضًا الاتصالات عن طريق (الشبكة اللاسلكية واسعة النطاق "Wireless Wide Area Network" WWAN) وعن طريق أجهزة المودم باستخدام بروتوكول نقطة إلى نقطة عبر إيثرنت (PPPOE). أخيرًا وليس آخرًا، يوفر التكامل مع العديد من أنواع الشبكات الخاصة الافتراضية (VPN) من خلال المكونات الإضافية المخصصة: SSH و OpenVPN و Cisco's VPNC و PPTP و Strongswan.

حزم *-network-manager، معظمها غير مثبتة افتراضياً.

لاحظ أنك تحتاج إلى الحزم الملحقة بـ gnome- لتتمكن من تكوينها من خلال واجهة المستخدم الرسومية.

2.1.5. بسطر الأوامر باستخدام حزم ifupdown

بدلاً من ذلك، عندما تفضل عدم استخدام (أو لا يمكنك الوصول إلى) سطح مكتب رسومي، يمكنك تكوين الشبكة عن طريق حزمة ifupdown المثبتة بالفعل، والتي تتضمن أدوات **ifup** و**ifdown**. تقوم هذه الأدوات بقراءة التعريفات من ملف التكوين **/etc/network/interfaces** والتي هي في صميم البرنامج النصي **/etc/init.d/networking** الذي يقوم بتكوين الشبكة في وقت الإقلاع.

يمكن إلغاء تكوين كل أجهزة الشبكة التي تتم إدارته بواسطة ifupdown في أي وقت باستخدام **ifdown** *network-device*. يمكنك بعد ذلك تعديل **/etc/network/interfaces** وإعادة عمل الشبكة احتياطياً (مع التكوين الجديد) باستخدام **ifup** *network-device*.

دعنا نلقي نظرة على ما يمكننا وضعه في ملف تكوين ifupdown. هناك توجيهان رئيسيان: **auto** *network-device*: الذي يخبر عن إعادة تهيئة لتكوين واجهة الشبكة تلقائيًا بمجرد توفرها. **iface** *network-device inet/inet6 type*: لتكوين واجهة معينة. على سبيل المثال، يبدو تكوين DHCP العادي كما يلي:

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet dhcp

لاحظ أن التكوين الخاص لجهاز الاسترجاع (loopback) يجب أن يكون موجودًا دائمًا في هذا الملف. لتكوين عنوان IP ثابت، يجب عليك تقديم المزيد من التفاصيل مثل عنوان IP والشبكة وعنوان IP الخاص بالبوابة:

```
auto eth0

iface eth0 inet static

address 192.168.0.3

netmask 255.255.255.0

broadcast 192.168.0.255

network 192.168.0.0

gateway 192.168.0.1
```

بالنسبة للواجهات اللاسلكية، يجب أن يكون لديك حزمة wpasupplicant (مضمنة في Kali افتراضيًا)، والتي توفر العديد من خيارات **wpa-*** التي يمكن استخدامها في **/etc/network/interfaces.** ألق نظرة على /usr/share/doc/wpasupplicant/README.Debian.gz للحصول على أمثلة وشروحات. أكثر الخيارات شيوعًا هي: wpa-ssid (الذي يحدد اسم الشبكة اللاسلكية للانضمام).

و wpa-psk (الذي يحدد كلمة المرور أو المفتاح الذي يحمي الشبكة).

iface wlan0 inet dhcp

wpa-ssid *MyNetWork*

wpa-psk *plaintextsecret*

3.1.5. على سطر الأوامر باستخدام *systemd-networkd*

على الرغم من أن *ifupdown* هي الأداة التاريخية لدبيان، ولكنها لا تزال هي الأداة الافتراضية للخادم أو أي تثبيتات أخرى بسيطة، إلا أن هناك أداة أحدث تستحق التجربة وهي : *systemd-networkd*. ودمجها مع نظام init *systemd* يجعلها خيارًا جذابًا للغاية. لا يقتصر الأمر على التوزيعات المستندة على دبيان (على عكس *ifupdown*) وقد تم تصميمه ليكون صغيرًا جدًا وفعالًا وسهل التكوين نسبيًا إذا فهمت بنية ملفات وحدة النظام. يعد هذا خيارًا جذابًا بشكل خاص إذا كنت تعتقد أنه يصعب تهيئة *NetworkManager*.

يمكنك تكوين **systemd-networkd** عن طريق وضع ملفات **network**. في المجلد **/etc/systemd/network/**. بدلاً من ذلك، يمكنك استخدام **/lib/systemd/network/** لملفات الحزم أو **/run/systemd/network/** للملفات التي تم إنشاؤها في وقت التشغيل. تم توثيق تنسيق هذه الملفات في systemd.network(5). يشير قسم **Match** إلى واجهات الشبكة التي ينطبق عليها التكوين. يمكنك تحديد الواجهة بعدة طرق، بما في ذلك عن طريق عنوان التحكم في الوصول إلى الوسائط (MAC) أو نوع الجهاز. يحدد قسم **Network** تكوين الشبكة.

مثال 1.5 التكوين الثابت في **/etc/systemd/network/50-static.network**

```
[Match]

Name=enp2s0

[Network]

Address=192.168.0.15/24

Gateway=192.168.0.1

DNS=8.8.8.8
```

مثال 2.5 التكوين المستند على DHCP في **etc/systemd/network/80-/dhcp.network**

```
[Match]
Name=en*
[Network]
DHCP=yes
```

لاحظ أنه تم تعطيل **system-networkd** بشكل افتراضي، لذلك إذا كنت ترغب في استخدامه، يجب عليك تمكينه. يعتمد أيضًا على **systemd-resolved** من أجل التكامل الصحيح لدقة DNS، الأمر الذي يتطلب منك استبدال ملف **etc/resolv.conf/** بوصله رمزية لـ **run/system/resolve/resolv.conf/**، والذي تم إدارته بواسطة **systemd-resolved.**

```
systemctl enable systemd-networkd
systemctl enable systemd-resolved
systemctl start systemd-networkd
systemctl start systemd-resolved
ln -sf /run/system/resolve/resolv.conf /etc/resolv.conf
```

على الرغم من أن **systemd-networkd** يعاني من بعض القيود، مثل عدم وجود دعم متكامل للشبكات اللاسلكية، يمكنك الاعتماد على تكوين **wpa_supplicant** خارجي موجود مسبقًا للدعم اللاسلكي. ومع ذلك، فهي مفيدة بشكل خاص في الـ containers والآلات الافتراضية "virtual machines"والتي تم تطويرها في الأصل للبيئات التي تعتمد فيها تهيئة شبكة الـ containers على تكوين شبكة مضيفها. في هذا السيناريو، يسهل **systemd-networkd** إدارة كلا الجانبين بطريقة منسقة مع الاستمرار في دعم جميع أنواع أجهزة الشبكة الافتراضية التي قد تحتاجها في هذا النوع من السيناريو انظر (5)systemd.netdev.

2.5. إدارة مستخدمي Unix ومجموعات Unix

تتكون قاعدة بيانات مستخدمي ومجموعات يونكس من ملفات نصية **/etc/passwd** (قائمة المستخدمين)، **/etc/shadow** (كلمات مرور مشفرة للمستخدمين)، **/etc/group** (قائمة المجموعات)، و **/etc/gshadow** (كلمات مرور مشفرة للمجموعات). تنسيقاتها موثقة في passwd (5) و shadow (5) و group (5) و gshadow (5) على التوالي. بينما يمكن تحرير هذه الملفات يدويًا باستخدام أدوات مثل **vipw** و **vigr**، هناك أدوات ذات مستوى أعلى لإجراء العمليات الأكثر شيوعًا.

استخدام getent لاستشارة قاعدة بيانات المستخدم

يتحقق الأمر **getent** (get entries) من قواعد بيانات النظام (بما في ذلك قواعد البيانات الخاصة بالمستخدمين والمجموعات) باستخدام وظائف المكتبة المناسبة، والتي بدورها تستدعي وحدات خدمة تبديل الاسم (NSS) المكونة في الملف /etc/nsswitch.conf. يأخذ الأمر مدخل أو اثنتين: اسم قاعدة البيانات للتحقق، ومفتاح بحث محتمل. وبالتالي، فإن الأمر **getent passwd** kaliuser1 سيعيد المعلومات من قاعدة بيانات المستخدم المتعلقة بالمستخدم kaliuser1.

```
root@kali:~# getent passwd kaliuser1
kaliuser1:x:1001:1001:Kali User,4444,123-867-5309,321-867-5309:/home/kaliuser1:/bin/bash
```

١.٢.٥. إنشاء حسابات المستخدمين

قد تحتاج أحيانا إلى إنشاء حسابات لأسباب مختلفة، خاصة إذا كنت تستخدم Kali كنظام تشغيل أساسي. الطريقة الأكثر شيوعًا لإضافة مستخدم هي الأمر **adduser**، الذي يطلب مدخل مطلوب وهو: اسم المستخدم؛ للمستخدم الجديد الذي ترغب في إنشائه.

يطرح أمر **adduser** بعض الأسئلة قبل إنشاء الحساب ولكن استخدامه واضح إلى حد ما. يتضمن ملف التكوين الخاص به، **/etc/adduser.conf**، العديد من الإعدادات المثيرة للاهتمام. يمكنك، على سبيل المثال، تحديد نطاق معرفات المستخدم (UIDs) التي يمكن استخدامها، وإملاء ما إذا كان المستخدمون يشتركون في مجموعة مشتركة أم لا، وتحديد الصدفات الافتراضية، والمزيد.

يؤدي إنشاء حساب إلى تشغيل محتوى المجلد الرئيسي للمستخدم بمحتويات النموذج **/etc/skel/**. يوفر ذلك للمستخدم مجموعة من المجلدات القياسية وملفات التكوين.

في بعض الحالات، سيكون من المفيد إضافة مستخدم إلى مجموعة (بخلاف المجموعة الرئيسية الافتراضية) لمنح أذونات إضافية. على سبيل المثال، المستخدم الذي تم تضمينه في مجموعة *sudo* لديه امتيازات إدارية كاملة من خلال الأمر **sudo**. يمكن تحقيق ذلك باستخدام أمر مثل: **adduser** *user group*.

٢.٢.٥. تعديل حساب موجود أو كلمة مرور

تسمح الأوامر التالية بتعديل المعلومات المخزنة في حقول محددة من قواعد بيانات المستخدم:

passwd - يسمح للمستخدم العادي بتغيير كلمة المرور الخاصة به، والتي بدورها تقوم بتحديث ملف **/etc/shadow**. || أو كلمة مرور مستخدم أخر، مثلا: sudo passwd *username*||

chfn— (change full name) ، المحجوز للمستخدم الفائق (الجذر)، يعدل حقل **GECOS**، أو حقل "معلومات عامة".

chsh — (change shell) يغير واجهة تسجيل دخول المستخدم. ومع ذلك، ستقتصر الخيارات المتاحة على تلك المدرجة في **/etc/shells**؛ المسؤول، من ناحية أخرى، غير ملزم بهذا التقييد ويمكنه تعيين shell لأي برنامج تم اختياره.

chage — (change age) يسمح للمسؤول بتغيير إعدادات انتهاء صلاحية كلمة المرور بتمرير اسم المستخدم كمدخل أو سرد الإعدادات الحالية باستخدام الخيار user **-l**. بدلاً من ذلك، يمكنك أيضًا فرض انتهاء صلاحية كلمة المرور باستخدام الأمر user **passwd -e**، مما يجبر المستخدم على تغيير كلمة المرور الخاصة به في المرة التالية التي يقوم فيها بتسجيل الدخول.

٣.٢.٥. تعطيل حساب

قد تجد نفسك بحاجة إلى تعطيل حساب (حظر مستخدم) كإجراء تأديبي، لأغراض التحقيق، أو ببساطة في حالة الغياب المطول أو النهائي للمستخدم. يعني الحساب المعطل أن المستخدم لا يمكنه تسجيل الدخول أو الوصول إلى الجهاز. يظل الحساب كما هو على الجهاز ولا يتم حذف أي ملفات أو بيانات؛ ببساطة لا يمكن الوصول إليها. يتم تحقيق ذلك باستخدام الأمر **passwd** *user* **-l** (القفل "lock"). تتم إعادة تمكين الحساب بطريقة مماثلة، مع الخيار **-u** (إلغاء القفل).

--||--

لقفل الحساب: `passwd -l user`

لإلغاء قفل الحساب: `passwd --unlock user`

لحذف كلمة المرور: `passwd --delete user`

وغيره .. تحقق من `man passwd` وانظر للخيارات المتاحة.

--||--

٤.٢.٥. إدارة مجموعات يونكس

يضيف الأمر **addgroup** مجموعة و **delgroup** يحذف مجموعة، يعدل الأمر **groupmod** معلومات المجموعة (رقم تعريفها **gid**- أو معرفها). يقوم الأمر *group* **gpasswd** بتغيير كلمة مرور المجموعة، بينما يقوم الأمر **gpasswd -r** *group* بحذفها.

العمل على عدة مجموعات

قد يكون كل مستخدم عضوا في العديد من المجموعات. يتم إنشاء المجموعة الرئيسية للمستخدم بشكل افتراضي أثناء التكوين الأولي للمستخدم. بشكل افتراضي، ينتمي كل ملف ينشئه المستخدم إلى المستخدم وكذلك إلى المجموعة الرئيسية للمستخدم. هذا ليس مرغوبًا دائمًا؛ على سبيل المثال، عندما يحتاج المستخدم للعمل في مجلد مشترك من قبل مجموعة غير مجموعته الرئيسية. في هذه الحالة، يحتاج المستخدم إلى تغيير المجموعات باستخدام أحد الأوامر التالية: **newgrp**، الذي يبدأ بصدفة جديدة، أو **sg**، والذي يقوم ببساطة بتنفيذ أمر باستخدام المجموعة البديلة المزودة. تسمح هذه الأوامر أيضًا للمستخدم بالانضمام إلى مجموعة لا ينتمي إليها حاليًا. إذا كانت المجموعة محمية بكلمة مرور، فسوف تحتاج إلى توفير كلمة المرور المناسبة قبل تنفيذ الأمر.

بدلاً من ذلك، يمكن للمستخدم تعيين بت **setgid** في المجلد، مما يؤدي إلى أن تنتمي الملفات التي تم إنشاؤها في هذا المجلد تلقائيًا إلى المجموعة الصحيحة.

يعرض الأمر **id** الحالة الحالية للمستخدم، مع معرفه الشخصي (متغير uid)، والمجموعة الرئيسية الحالية (متغير gid)، وقائمة المجموعات التي ينتمون إليها (متغير groups).

٣.٥. تكوين الخدمات

في هذا القسم، سنلقي نظرة على الخدمات (تسمى أحيانًا daemons)، أو البرامج التي تعمل كعمليات في الخلفية وتؤدي وظائف متنوعة للنظام. سنبدأ بمناقشة ملفات التكوين وسنشرع في شرح كيفية عمل بعض الخدمات المهمة (مثل SSH وPostgreSQL وApache) وكيف يمكن تكوينها.

١.٣.٥. تكوين برنامج معين

عندما تريد تكوين حزمة غير معروفة، يجب عليك متابعة هذه المراحل. أولاً، يجب عليك قراءة ما وثقه مشرف الحزمة. يعد ملف **/usr/share/doc/***package***/README.Debian** مكانًا جيدًا للبدء. غالبًا ما يحتوي هذا الملف على معلومات حول الحزم، بما في ذلك المؤشرات التي قد تحيلك إلى وثائق أخرى. غالبًا ما توفر لك الكثير من الوقت، وتجنب الكثير من الإحباط، من خلال قراءة هذا الملف أولاً لأنه غالبًا ما يوضح تفاصيل الأخطاء والحلول الأكثر شيوعًا لمعظم المشاكل الشائعة.

بعد ذلك، يجب عليك إلقاء نظرة على الوثائق الرسمية للبرنامج. راجع القسم ١.٦. "مصادر التوثيق" للحصول على نصائح حول كيفية العثور على مصادر توثيق مختلفة. يعطي الأمر:

dpkg -L *package*

قائمة بالملفات المضمنة في الحزمة؛ لذلك يمكنك تحديد الوثائق المتاحة بسرعة (بالإضافة إلى ملفات التكوين الموجودة في /etc/). أيضًا الأمر: **dpkg -s** *package* يعرض البيانات الوصفية للحزمة وتعرض أي حزم ممكنة موصى بها أو مقترحة؛ هناك، يمكنك العثور على وثائق أو أداة مساعدة من شأنها تسهيل تكوين البرنامج.

أخيرًا، غالبًا ما يتم توثيق ملفات التكوين ذاتيًا من خلال العديد من التعليقات التفسيرية التي توضح بالتفصيل مختلف القيم الممكنة لكل إعداد تكوين. في بعض الحالات، يمكنك الحصول على البرنامج وتشغيله عن طريق إلغاء تعليق سطر واحد فقط في ملف التكوين. في حالات أخرى، يتم توفير أمثلة لملفات التكوين في المجلد **/usr/share/doc/*package*/examples/**. قد تكون بمثابة أساس لملف التكوين الخاص بك.

٢.٣.٥. تكوين SSH لتسجيلات الدخول عن بعد

يسمح لك SSH بتسجيل الدخول إلى الجهاز عن بُعد أو نقل الملفات أو تنفيذ الأوامر. الأداة القياسية هي (ssh) وأما الخدمة (sshd) للاتصال بالأجهزة عن بعد.

أثناء تثبيت حزمة opensh-server افتراضيًا، يتم تعطيل خدمة SSH افتراضيًا وبالتالي لا يتم تشغيلها في وقت الإقلاع. يمكنك بدء تشغيل خدمة SSH يدويًا بكتابة الأمر:

```
systemctl start ssh
```

أو تهيئتها للبدء في وقت الإقلاع باستخدام الأمر:

```
systemctl enable ssh
```

خدمة SSH لها تكوين افتراضي معقول نسبيًا، ولكن نظرًا لقدراتها القوية وطبيعتها الحساسة، من الجيد معرفة ما يمكنك القيام به في ملف التكوين الخاص بها، **/etc/ssh/sshd_config/**. تم توثيق جميع الخيارات في (5) sshd_config.

يعطل التكوين الافتراضي عمليات تسجيل الدخول المستندة إلى كلمة المرور للمستخدم الجذر، مما يعني أنه يجب عليك أولاً إعداد مفاتيح SSH باستخدام **ssh-keygen**. يمكنك تمديد هذا إلى جميع المستخدمين عن طريق تعيين **PasswordAuthentication** إلى **no**، أو يمكنك رفع هذا القيد عن طريق تغيير **PermitRootLogin** إلى **yes** (بدلاً من كلمة المرور المحظورة الافتراضية). تستمع خدمة SSH بشكل افتراضي على المنفذ (port) 22 ولكن يمكنك تغيير ذلك باستخدام توجيه **Port**.

لتطبيق الإعدادات الجديدة، يجب كتابة الأمر **systemctl reload ssh**.

توليد مفاتيح مضيف SSH جديدة

يحتوي كل خادم SSH على مفاتيح التشفير الخاصة به؛ يتم تسميتها "مفاتيح مضيف SSH" ويتم تخزينها في *_etc/ssh/ssh_host/. يجب الحفاظ على خصوصيتها إذا كنت تريد السرية ولا يجب مشاركتها مع أجهزة متعددة.

عندما تقوم بتثبيت النظام الخاص بك عن طريق نسخ صورة قرص كاملة (بدلاً من استخدام برنامج debian-installer)، فقد تحتوي الصورة على مفاتيح مضيف SSH تم إنشاؤها مسبقًا والتي يجب عليك استبدالها بمفاتيح تم إنشاؤها حديثًا. من المحتمل أن تأتي الصورة أيضًا بكلمة مرور جذر افتراضية تريد إعادة تعيينها في نفس الوقت. يمكنك القيام بكل ذلك باستخدام الأوامر التالية:

```
#passwd [...]
#rm /etc/ssh/ssh_host*_
#dpkg-reconfigure openssh-server
#service ssh restart
```

٣.٣.٥. تكوين قواعد بيانات PostgreSQL

PostgreSQL هو خادم قاعدة بيانات. نادرًا ما يكون مفيدًا من تلقاء نفسه ولكن يتم استخدامه من قبل العديد من الخدمات الأخرى لتخزين البيانات. ستصل هذه الخدمات بشكل عام إلى خادم قاعدة البيانات عبر الشبكة وتتطلب عادة بيانات اعتماد المصادقة لتكون قادرة على الاتصال. وبالتالي يتطلب إعداد هذه الخدمات إنشاء قواعد بيانات PostgreSQL وحسابات المستخدمين مع الامتيازات المناسبة لقاعدة البيانات. حتى نتمكن من القيام بذلك، نحتاج إلى تشغيل الخدمة، لذا دعنا نبدأ بالأمر:

```
systemctl start postgresql
```

دعم العديد من إصدارات PostgreSQL

تسمح حزمة PostgreSQL بتثبيت نسخ متعددة من خادم قاعدة البيانات. من الممكن أيضًا التعامل مع *clusters* متعددة (cluster هي مجموعة من قواعد البيانات التي يقدمها نفس مدير البريد "postmaster"). لتحقيق ذلك، يتم تخزين ملفات التكوين في /etc/postgresql/*version*/*cluster-name*/.

من أجل تشغيل الـ clusters جنبًا إلى جنب، يتم تعيين رقم المنفذ التالي المتاح لكل مجموعة جديدة (عادةً ٥٤٣٣ للمجموعة الثانية). ملف postgresql.service عبارة عن صدفة فارغة، مما يجعل من السهل العمل على كل المجموعات "clusters" معًا حيث أن لكل مجموعة وحدتها الخاصة (postgresql@*version-cluster*.service).

١.٣.٣.٥. نوع الاتصال ومصادقة العميل

بشكل افتراضي، يستمع PostgreSQL للاتصالات الواردة بطريقتين: على منفذ TCP 5432 لواجهة المضيف المحلي وعلى المقبس " socket" المستند للملفات **/var/run/postgresql/.s.PGSQL.5432**. يمكن تكوين ذلك في **postgresql.conf** مع توجيهات متنوعة: **listen_addresses** للعنوان الذي تريد الاستماع منه، **port** لمنفذ TCP، و **unix_socket_directories** لتعريف المجلد حيث يتم إنشاء المقابس المستندة إلى الملفات.

اعتماداً على كيفية الاتصال، يتم مصادقة العملاء بطرق مختلفة. يحدد ملف التكوين **pg_hba.conf** من الذي يسمح له بالاتصال على كل مقبس وكيفية مصادقته. بشكل افتراضي، تستخدم الاتصالات على مأخذ التوصيل المستند إلى الملفات حساب مستخدم Unix كاسم مستخدم PosgreSQL، ويفترض أنه لا توجد مصادقة أخرى مطلوبة. في اتصال TCP، يطلب PostgreSQL من المستخدم المصادقة باستخدام اسم مستخدم وكلمة مرور (على الرغم من أنه ليس اسم مستخدم/كلمة مرور Unix ولكن بدلاً من ذلك واحد يديره PostgreSQL نفسه).

مستخدم **postgres** خاص ولديه امتيازات إدارية كاملة على جميع قواعد البيانات. سنستخدم هذه الهوية لإنشاء مستخدمين جدد وقواعد بيانات جديدة.

٢.٣.٣.٥. إنشاء المستخدمين وقواعد البيانات

يضيف الأمر **createuser** مستخدمًا جديدًا ويزيل **dropuser** المستخدم. وبالمثل، يضيف الأمر **createdb** قاعدة بيانات جديدة ويزيل **dropdb** قاعدة بيانات. كل من هذه الأوامر لها صفحات يدوية خاصة بها ولكننا سنناقش بعض الخيارات هنا. يعمل كل أمر على الكتلة " cluster" الافتراضية (يعمل على المنفذ 5432) ولكن يمكنك تمرير:

--port=*port*

لتعديل المستخدمين وقواعد البيانات الخاصة بالكتلة البديلة.

يجب أن تتصل هذه الأوامر بخادم PostgreSQL للقيام بعملهم ويجب أن تتم مصادقتهم كمستخدم يتمتع بامتيازات كافية ليتمكنوا من تنفيذ العملية المحددة. أسهل طريقة لتحقيق ذلك هي استخدام حساب Unix **postgres** والاتصال عبر المقبس المستند إلى الملفات " file-based socket":

```
# su - postgres
$ createuser -P king_phisher
Enter password for new role:
Enter it again:
$ createdb -T template0 -E UTF-8 -O king_phisher king_phisher
$ exit
```

في المثال السابق، يطلب الخيار **P-** من الأمر **createuser** تعيين كلمة مرور جديدة لحساب **king_phisher** بمجرد إنشائه. بالنظر إلى الأمر **createdb**، يحدد الخيار **O-** المستخدم الذي يمتلك قاعدة البيانات الجديدة (الذي يتمتع بالتالي بحقوق كاملة لإنشاء الجداول ومنح الأذونات وما إلى ذلك). نريد أيضًا أن نكون قادرين على استخدام سلاسل Unicode، لذلك نضيف الخيار **E UTF-8-** لضبط الترميز، والذي بدوره يتطلب منا استخدام خيار **T-** لاختيار قالب قاعدة بيانات آخر.

يمكننا الآن اختبار إمكانية الاتصال بقاعدة البيانات عبر الاستماع إلى مأخذ التوصيل على المضيف المحلي (**-h localhost**) كمستخدم king_phisher (**-U king_phisher**):

```
# psql -h localhost -U king_phisher king_phisher
Password for user king_phisher:
psql (9.5.2)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help. king_phisher=>
```

كما ترى، نجح الاتصال.

٣.٣.٣.٥. إدارة مجموعات PostgreSQL

أولاً، تجدر الإشارة إلى أن مفهوم "مجموعة -cluster– PostgreSQL" هو إضافة خاصة بـ Debian ولن تجد أي إشارة لهذا المصطلح في وثائق PostgreSQL الرسمية. من وجهة نظر أدوات PostgreSQL، فإن هذه المجموعة هي مجرد مثيل لخادم قاعدة بيانات يعمل على منفذ معين.

ومع ذلك، توفر حزمة ديبيان postgresql الشائعة أدوات متعددة لإدارة هذه المجموعات:

pg_createcluster, **pg_dropcluster**, **pg_ctlcluster**, **pg_upgradecluster**, **pg_renamecluster**, **pg_lsclusters.**

لن نغطي جميع هذه الأدوات هنا، ولكن يمكنك الرجوع إلى الصفحات اليدوية الخاصة بها لمزيد من المعلومات.

ما يجب أن تعرفه هو أنه عندما يتم تثبيت إصدار رئيسي جديد من PostgreSQL على نظامك، فإنه سيقوم بإنشاء مجموعة جديدة تعمل على المنفذ التالي (عادة 5433) وستستمر في استخدام الإصدار القديم حتى تقوم بترحيل قواعد البيانات الخاصة بك من المجموعة القديمة إلى الجديدة.

يمكنك استرداد قائمة بجميع المجموعات وحالتها باستخدام أمر: **pg_lsclusters.** الأهم من ذلك، يمكنك أتمتة ترحيل نظامك إلى أحدث إصدار من PostgreSQL باستخدام:

```
pg_upgradecluster old-version cluster-name
```

لكي ينجح هذا، قد تحتاج أولاً إلى إزالة نظام المجموعة (empty) الذي تم إنشاؤه من أجل الإصدار الجديد (باستخدام: **pg_dropcluster** *new-version cluster-name*). لا يتم إسقاط المجموعة القديمة في العملية، ولكن لن يتم بدء تشغيلها تلقائيًا أيضًا. يمكنك إسقاطها بمجرد التحقق من أن المجموعة التي تمت ترقيتها تعمل بشكل جيد.

٤.٣.٥. تكوين أباتشي

يشتمل التثبيت النموذجي لـ Kali Linux على خادم الويب Apache، الذي توفره حزمة apache2. كونها خدمة شبكة، يتم تعطيلها بشكل افتراضي. يمكنك تشغيله يدويًا باستخدام:

systemctl start apache2.

مع انتشار الكثير والكثير من تطبيقات الويب صار من المهم أن يكون لديك بعض المعرفة بـ Apache من أجل استضافة هذه التطبيقات، سواء للاستخدام المحلي أو لإتاحتها عبر الشبكة.

Apache هو خادم وحدات -modular server- ويتم تنفيذ العديد من الميزات بواسطة وحدات -modules- خارجية يقوم البرنامج الرئيسي بتحميلها أثناء التهيئة. يتيح التكوين الافتراضي فقط الوحدات -modules- الأكثر شيوعًا، ولكن تمكين الوحدات الجديدة يتم بسهولة عن طريق تشغيل *module* **a2enmod**. استخدم *module* **a2dismod** لتعطيل الوحدة. تقوم هذه البرامج في الواقع بإنشاء (أو حذف) روابط رمزية فقط في:

||**a2enmod** "**a**pache **2** **en**able **mod**ule".

a2dismod "**a**pache **2** **dis**able **mod**ule"||

/etc/apache2/mods-enabled/

مشيرة إلى الملفات الحقيقية (المخزنة في **/etc/apache2/mods-available/**).

هناك العديد من الوحدات المتاحة، ولكن هناك اثنتان تستحق النظر الأولي: PHP وSSL. يتم تنفيذ تطبيقات الويب المكتوبة باستخدام PHP بواسطة خادم الويب Apache بمساعدة الوحدة المخصصة التي توفرها حزمة libapache-mod-php، وعند تثبيتها تمكن الوحدة تلقائيا.

يتضمن Apache 2.4 وحدة SSL المطلوبة لـ HTTP الآمن (HTTPS) خارج الصندوق. يجب أولاً تمكينه باستخدام: **`a2enmod ssl`**، ثم يجب إضافة التوجيهات المطلوبة لملفات التكوين. يتوفر مثال التكوين في **/etc/apache2/sites-available/default-ssl.conf**. راجع http://httpd.apache.org/docs/2.4/mod/mod_ssl.html لمزيد من المعلومات.

يمكن العثور على القائمة الكاملة لوحدات Apache القياسية عبر الإنترنت في http://httpd.apache.org/docs/2.4/mod/index.html.

باستخدام التكوين الافتراضي، يستمع خادم الويب على المنفذ 80 (كما تم تكوينه في **`/etc/apache2/ports.conf`**)، وصفحات الخادم من المجلد **/var/www/html/** بشكل افتراضي (كما تم تكوينه في **/etc/apache2/sites-enabled/000-default.conf**).

٥.٣.٤.١. تكوين المضيفين الافتراضيين

المضيف الافتراضي هو هوية إضافية لخادم الويب. يمكن أن تخدم عملية أباتشي نفسها مواقع ويب متعددة (مثل www.kali.org و www.offensive-security.com) لأن طلبات HTTP تتضمن كلاً من اسم موقع الويب المطلوب وعنوان URL المحلي (تُعرف هذه الميزة باسم: *namebased virtual hosts*).

يتيح التكوين الافتراضي لـ Apache 2 تمكين name-based virtual hosts. بالإضافة إلى ذلك، يتم تعريف مضيف افتراضي افتراضيا في ملف **/etc/apache2/sites-enabled/000-default.conf**؛ سيتم استخدام هذا المضيف الافتراضي إذا لم يتم العثور على مضيف مطابق للطلب الذي أرسله العميل.

مهم

سيتم دائمًا تقديم الطلبات المتعلقة بالمضيفات الافتراضية غير المعروفة بواسطة المضيف الافتراضي المحدد أولا، ولهذا السبب تقوم الحزمة بشحن ملف تكوين **000-default.conf**، والذي يتم فرزه أولاً بين جميع الملفات الأخرى التي قد تقوم بإنشائها.

يتم بعد ذلك وصف كل مضيف افتراضي إضافي بواسطة ملف مخزن في ‎**/etc/apache2/sites-available/**‎. عادةً ما تتم تسمية الملف باسم موقع الويب متبوعًا بامتداد **conf**. (على سبيل المثال: ‎**www.example.com.conf**‎). يمكنك بعد ذلك تمكين المضيف الافتراضي الجديد باستخدام: ‎**a2ensite** *www.example.com*‎. فيما يلي الحد الأدنى من تكوين المستضيف الافتراضي لموقع ويب يتم تخزين ملفاته في ‎**/srv/www.example.com/www/**‎ (محدد بخيار **DocumentRoot**):

```
ServerName www.example.com
ServerAlias example.com
DocumentRoot /srv/www.example.com/www
```

قد تفكر أيضًا في إضافة توجيهات CustomLog و ErrorLog لتكوين Apache لإخراج سجلات الدخول في ملفات مخصصة للمضيف الافتراضي.

٢.٤.٣.٥. توجيهات شائعة الإستخدام

يستعرض هذا القسم بعض توجيهات تكوين Apache شائعة الاستخدام.

عادة ما يتضمن ملف التكوين الرئيسي العديد من كتل **Directory** -مجلد-، أنها تسمح بتحديد سلوكيات مختلفة للخادم حسب موقع الملف الذي يتم تقديمه. تتضمن مثل هذه الكتلة الشائعة **Options** و **AllowOverride**:

```
Options Includes FollowSymLinks
AllowOverride All
DirectoryIndex index.php index.html index.htm
```

يحتوي التوجيه **DirectoryIndex** على قائمة بالملفات التي يجب تجربتها عندما يطابق طلب العميل مجلدا. يتم استخدام أول ملف موجود في القائمة وإرساله كرد.

ويتبع توجيه **Options** قائمة من الخيارات للتمكين. تقوم القيمة **None** بتعطيل جميع الخيارات، وبالمثل، فإن **All** يمكّنهم جميعًا باستثناء **MultiViews**. تشمل الخيارات المتاحة:

- **ExecCGI** - يشير إلى أنه يمكن تنفيذ البرامج النصية CGI.
- **FollowSymLinks** - تخبر الخادم أنه يمكنه اتباع الروابط الرمزية، وأن الاستجابة يجب أن تحتوي على محتويات هدف هذه الروابط.

- ❖ **SymLinksIfOwnerMatch** - يخبر الخادم أيضًا باتباع الروابط الرمزية، ولكن فقط عندما يكون للرابط وهدفه المالك نفسه.
- ❖ **Includes**- يمكّن تضمين جانب الخادم -*Server Side Includes*- (SSI). هذه توجيهات مضمنة في صفحات HTML وتنفيذها على الفور لكل طلب.
- ❖ **Indexes**– تطلب من الخادم إدراج محتويات المجلد إذا كان طلب HTTP الذي أرسله العميل يشير إلى مجلد بدون ملف فهرس (أي عندما لا توجد ملفات مذكورة في توجيه **DirectoryIndex** في هذا المجلد).
- ❖ **MultiViews** - تتيح التفاوض -negotiation- على المحتوى؛ يمكن استخدام هذا من قبل الخادم لإرجاع صفحة ويب مطابقة للغة المفضلة كما تم تكوينه في المستعرض.

١.٢.٤.٣.٥. طلب المصادقة

في بعض الحالات، يجب تقييد الوصول إلى جزء من موقع ويب، لذلك يتم منح حق الوصول إلى المحتويات للمستخدمين الشرعيين فقط الذين يقدمون اسم مستخدم وكلمة مرور.

يحتوي ملف **htaccess.** على توجيهات تكوين Apache التي يتم فرضها في كل مرة يتعلق فيها الطلب بعنصر من المجلد حيث يتم تخزين ملف **htaccess.**. هذه التوجيهات متكررة، مما يوسع النطاق ليشمل جميع المجلدات الفرعية.

معظم التوجيهات التي يمكن أن تحدث في كتلة **Directory** قانونية أيضًا في ملف **htaccess.**. يسرد الأمر **AllowOverride** جميع الخيارات التي يمكن تمكينها أو تعطيلها عن طريق **htaccess.** الاستخدام الشائع لهذا الخيار هو تقييد **ExecCGI**، بحيث يختار المسؤول المستخدمين المسموح لهم بتشغيل البرامج تحت هوية خادم الويب (مستخدم الـ **www-data**).

مثال ٣.٥. **htaccess.** ملف يتطلب المصادقة

```
Require valid-user
AuthName "Private directory"
AuthType Basic
AuthUserFile /etc/apache2/authfiles/htpasswd-private
```

لا توفر المصادقة الأساسية -Basic- الأمان

> يمتع نظام المصادقة المستخدم في المثال السابق (Basic) بالحد الأدنى من الأمان حيث يتم إرسال كلمة المرور بنص واضح (يتم ترميزها فقط كـ *base64*، وهو ترميز بسيط بدلاً من أسلوب تشفير). وتجدر الإشارة أيضًا إلى أن المستندات التي تحميها هذه الآلية أيضًا تمر عبر الشبكة بشكل واضح. إذا كان الأمان مهمًا، فيجب تشفير جلسة HTTP بالكامل باستخدام طبقة النقل الآمنة (TLS).

يحتوي الملف **/etc/apache2/authfiles/htpasswd-private** على قائمة بالمستخدمين وكلمات المرور، يتم التلاعب بها عادة باستخدام الأمر **htpasswd**. على سبيل المثال، يتم استخدام الأمر التالي لإضافة مستخدم أو تغيير كلمة المرور الخاصة به:

```
# htpasswd /etc/apache2/authfiles/htpasswd-private user
New password: Re-type new password: Adding password for user user
```

٢.٢.٤.٣.٥. تقييد الوصول

يتحكم التوجيه **Require** في قيود الوصول إلى المجلد (والمجلدات الفرعية الخاصة به، بشكل متكرر).

يمكن استخدامه لتقييد الوصول على أساس العديد من المعايير؛ سنتوقف عند وصف تقييد الوصول استنادًا إلى عنوان IP للعميل ولكن يمكن جعله أكثر قوة من ذلك، خاصة عندما يتم دمج العديد من التوجيهات المطلوبة -**Require**- داخل كتلة **RequireAll**،

على سبيل المثال، يمكنك تقييد الوصول إلى الشبكة المحلية باستخدام التوجيه التالي:

```
Require ip 192.168.0.0/16
```

4.5. إدارة الخوادم

يستخدم كالي **systemd** كنظام خاص به، وهو ليس مسؤولًا فقط عن تسلسل الإقلاع، ولكنه يعمل أيضًا بشكل دائم كمدير خوادم كامل الميزات لبدء ومراقبة الخدمات.

يمكن الاستعلام عن **systemd** والتحكم فيه باستخدام **systemctl**. بدون أي مدخلات، يقوم بتشغيل الأمر **systemctl list-units** الذي ينتج قائمة *بالوحدات* النشطة. إذا قمت بتشغيل **systemctl status**، يعرض الإخراج نظرة عامة هرمية للخدمات قيد التشغيل. بمقارنة كل من المخرجات، ترى على الفور أن هناك أنواعًا متعددة من الوحدات وأن الخدمات واحدة فقط بينها.

يتم تمثيل كل خدمة *بوحدة خدمة -service unit-*، والتي يتم وصفها بملف خدمة يتم شحنها عادةً في **/lib/systemd/system/** (أو **/run/systemd/system/**، أو **/etc/systemd/system/** ؛ يتم إدراجها عن طريق زيادة ترتيب الأهمية، وآخر واحد يفوز). ربما يتم تعديل كل منها عن طريق ملفات *service-name*.**service.d/*.conf** أخرى في نفس مجموعة المجلدات. ملفات الوحدات هذه هي ملفات نصية عادية تعرف بامتداد "*.ini" أحيانا المعروفة في Microsoft Windows، مع أزواج *key = value* مجمعة بين رؤوس [*section*]. نرى هنا ملف خادم بسيط لـ **/lib/systemd/system/ssh.service**:

```
[Unit]
Description=OpenBSD Secure Shell server
After=network.target auditd.service
```

```
ConditionPathExists=!/etc/ssh/sshd_not_to_be_run

[Service]
EnvironmentFile=-/etc/default/ssh
ExecStart=/usr/sbin/sshd -D $SSHD_OPTS
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartPreventExitStatus=255
Type=notify

[Install]
WantedBy=multi-user.target
Alias=sshd.service
```

الوحدات المستهدفة هي جزء آخر من تصميم النظام. تمثل الحالة المرغوبة التي تريد تحقيقها من حيث الوحدات النشطة (مما يعني خدمة جارية في حالة وحدات الخدمة). وهي موجودة بشكل أساسي كوسيلة لتجميع التبعيات على الوحدات الأخرى. عندما يبدأ النظام، فإنه يمكّن الوحدات المطلوبة للوصول إلى **default.target** (وهي وصلة رمزية لـ **graphical.target** والذي يعتمد بدوره على **multi-user.target**). لذلك يتم تنشيط جميع تبعيات تلك الأهداف أثناء الإقلاع.

يتم التعبير عن هذه التبعيات بتوجيه **Wants** على الوحدة المستهدفة. ولكن ليس عليك تعديل الوحدة المستهدفة لإضافة تبعيات جديدة، يمكنك أيضًا إنشاء وصلة رمزية تشير للوحدة التابعة في المجلد **/etc/systemd/system/***target-name***.target.wants/**.

وهذا بالضبط ما يفعله *foo.service* **systemctl enable**. عندما تقوم بتمكين خدمة، فأنت تخبر systemd أن يضيف تبعية على الأهداف المدرجة في إدخال **WantedBy** لقسم [**install**] لملف وحدة الخدمة. عكس ذلك، يقوم **systemctl** *foo.service* **disable** بتعطيل نفس الوصلة الرمزية وبالتالي التبعية.

أمرا **enable** و **disable** لا تغير أي شيء يتعلق بالحالة الحالية للخدمات. إنهم تؤثران فقط على ما سيحدث في الإقلاع التالي. إذا كنت ترغب في تشغيل الخدمة على الفور، فيجب عليك تشغيل: *foo.service* **systemctl start**. على العكس من ذلك، يمكنك إيقافه من خلال *foo.service* **systemctl stop**. يمكنك أيضًا فحص الحالة الحالية للخدمة باستخدام: *foo.service* **systemctl status**، والتي تتضمن بشكل مفيد أحدث أسطر من السجل المرتبط. بعد تغيير تكوين الخدمة، قد ترغب في إعادة تحميلها أو إعادة تشغيلها: تتم هذه العمليات باستخدام: **systemctl** *foo.service* **reload** و *foo.service* **systemctl restart** على التوالي.

```
# systemctl status postgresql
```

● postgresql.service - PostgreSQL RDBMS

Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)

Active: inactive (dead)

```
# ls -al /etc/systemd/system/multi-user.target.wants/postgresql.service
```

ls: cannot access '/etc/systemd/system/multi-user.target.wants/postgresql.service': No such file or directory

systemctl enable postgresql

[...]

ls -al /etc/systemd/system/multi-user.target.wants/postgresql.service

lrwxrwxrwx 1 root root 38 Apr 21 16:21 /etc/systemd/system/multi-user.target.wants/postgresql.service -> /lib/systemd/system/postgresql.service

systemctl status postgresql

● postgresql.service - PostgreSQL RDBMS

Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: disabled)

Active: inactive (dead)

systemctl start postgresql

systemctl status postgresql

● postgresql.service - PostgreSQL RDBMS

Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: disabled)

Active: active (exited) since Thu 2016-04-21 16:22:29 EDT; 2s ago

Process: 6355 ExecStart=/bin/true (code=exited, status=0/SUCCESS)

Main PID: 6355 (code=exited, status=0/SUCCESS)

Apr 21 16:22:29 kali-rolling systemd[1]: Starting PostgreSQL RDBMS...

Apr 21 16:22:29 kali-rolling systemd[1]: Started PostgreSQL RDBMS.

٥.٥. الملخص

تعلمنا في هذا الفصل كيفية تكوين Kali Linux. قمنا بتكوين إعدادات الشبكة، وتحدثنا عن المستخدمين والمجموعات، وناقشنا كيفية إنشاء وتعديل حسابات المستخدمين، وتعيين كلمات المرور، وتعطيل الحسابات، وإدارة المجموعات. أخيرًا، ناقشنا الخدمات وشرحنا كيفية إعداد الخدمات العامة وصيانتها، وتحديدًا SSH و PostgreSQL و Apache.

نصائح الملخص:

❖ في التثبيت النموذجي لسطح المكتب، سيكون لديك NetworkManager مثبتاً بالفعل ويمكن التحكم فيه وتكوينه من خلال مركز التحكم في GNOME ومن خلال القائمة العلوية اليمنى.

❖ يمكنك تكوين الشبكة من خلال سطر الأوامر باستخدام أدوات **ifup** و **ifdown**، التي تقرأ تعليماتها من ملف التكوين **/etc/network/interfaces**. أداة أحدث، *systemd-networkd* تعمل مع نظام *systemd* init.

❖ بشكل افتراضي، تتكون قاعدة بيانات مستخدمي ومجموعات Unix من ملفات نصية **/etc/passwd** (قائمة المستخدمين)، **/etc/shadow** (كلمات المرور المشفرة للمستخدمين)، **/etc/group** (قائمة المجموعات)، و **/etc/gshadow** (كلمات المرور المشفرة للمجموعات).

❖ يمكنك استخدام الأمر **getent** لاستشارة قاعدة بيانات المستخدم وقواعد بيانات النظام الأخرى.

❖ يطرح أمر **adduser** بعض الأسئلة قبل إنشاء الحساب، ولكنها الطريقة المباشرة لإنشاء حساب مستخدم جديد.

❖ يمكن استخدام عدة أوامر لتعديل حقول معينة في قاعدة بيانات المستخدم بما في ذلك: **passwd** (تغيير كلمة المرور)، **chfn** (تغيير الاسم الكامل و**GECOS**، أو حقل المعلومات العامة)، **chsh** (تغيير تسجيل الدخول الصدفة)، **chage** (تغيير عمر كلمة المرور)،و **passwd -e** *user* (يجبر المستخدم على تغيير كلمة المرور الخاصة به في المرة التالية التي يقوم فيها بتسجيل الدخول).

❖ يمكن لكل مستخدم أن يكون عضوا في مجموعة واحدة أو مجموعات متعددة. يمكن استخدام عدة أوامر لتعديل هوية المجموعة: يغير **newgrp** معرف المجموعة الحالي، **sg** ينفذ أمرًا باستخدام المجموعة البديلة المزودة، ويمكن وضع بت **setgid** في مجلد، مما يؤدي إلى أن تنتمي الملفات التي تم إنشاؤها في هذا المجلد تلقائيًا إلى المجموعة الصحيحة. بالإضافة إلى ذلك، يعرض الأمر **id** الحالة الحالية للمستخدم بما في ذلك قائمة بعضوية مجموعته.

❖ يمكنك بدء SSH يدويًا باستخدام **systemctl start ssh** أو تمكينه بشكل دائم باستخدام **systemctl enable ssh**. يعطل التكوين الافتراضي عمليات تسجيل الدخول المستندة إلى كلمة المرور للمستخدم الجذر، مما يعني أنه يجب عليك أولاً إعداد مفاتيح SSH باستخدام **ssh-keygen**.

❖ PostgreSQL هو خادم قاعدة بيانات. نادرًا ما يكون مفيدًا من تلقاء نفسه ولكن يتم استخدامه من قبل العديد من الخدمات الأخرى لتخزين البيانات.

❖ يشتمل التثبيت النموذجي لـ Kali Linux على خادم الويب Apache، الذي توفره حزمة apache2. كونها خدمة شبكة، يتم تعطيلها بشكل افتراضي. يمكنك تشغيله يدويًا باستخدام **systemctl start apache2**.

❖ من خلال التكوين الافتراضي، يستمع Apache على المنفذ 80 (كما تم تكوينه في **/etc/apache2/ports.conf**)، ويقدم صفحات من المجلد **/var/www/html/** افتراضيًا (كما تم تكوينه في **/etc/apache2/sites-enabled/000-default.conf**).

الآن بعد أن تعاملنا مع أساسيات Linux وتثبيت Kali Linux وتكوينه، دعنا نناقش كيفية تحرّي الخلل وإصلاحه وتعليمك بعض الأدوات والحيل لإعادتك للعمل عند مواجهة المشاكل.

التمرين الأول، الفصل الخامس - تكوين المستخدمين

١. قم بإنشاء حساب مستخدم قياسي. أضف المستخدم الجديد إلى مجموعة "sudo"

الإجابة:

```
adduser username
passwd username
usermod -a -G sudo username
chsh -s /bin/bash username
```

التمرين الثاني، للفصل الخامس - تكوين الشبكة

٢. أوقف خدمة Network Manager وقم بتعطيلها بالكامل في وقت الإقلاع.

٣. تكوين جهاز Kali الخاص بك لـ DHCP على eth0

٤. إنزال واجهة eth0.

٥. اتصل بالشبكة اللاسلكية باستخدام دونجل USB اللاسلكي الخاص بك عن طريق تكوين /etc/network/interfaces وفقًا لذلك.

الإجابة:

١. مدير الشبكة مفيد، ولكن في اختبار الإختراق تحتاج حقًا إلى الاستيلاء على واجهاتك وثنيها حسب إرادتك دون أي مفاجآت. لإيقاف Network Manager وتعطيله في وقت الإقلاع:

```
systemctl stop NetworkManager.service
systemctl disable NetworkManager.service
```

يمكنك التحقق من حالة الواجهات المُدارة في Network Manager من خلال:

```
nmcli dev status
```

نصيحة احترافية: أوقف مدير الشبكة من خلال إضافة dns-servers إلى ملف /etc/resolv.conf:

```
nano /etc/NetworkManager/NetworkManager.conf
```

أضف dns=none لقسم [main].

٢. اضبط eth0 لـ DHCP. قم بتغير ملف /etc/network/interfaces لتضمين:

```
auto eth0
iface eth0 inet dhcp
```

يمكنك أيضًا إعداد عنوان ثابت باستخدام ما يلي:

```
auto eth0

iface eth0 inet static

    address 192.168.1.160

    netmask 255.255.255.0

    gateway 192.168.1.1
```

٣. إنزال واجهة eth0:

```
ifconfig eth0 down
```

٤. الاتصال بشبكة لاسلكية. لاحظ أنه إذا كنت في جهاز إفتراضي، فستحتاج إلى محول لاسلكي USB. يفترض هذا المثال WPA2.Generate psk باستخدام الأمر التالي:

```
wpa_passphrase myssid wpa-password
```

الآن قم بإدراج PSK مع ما يلي داخل ملف /etc/network/interfaces:

```
auto wlan0

iface wlan0 inet dhcp

   wpa-ssid myssid

   wpa-psk {whatever the psk hash was}
```

قم بتدوير الواجهة:

```
ifup wlan0
```

التمرين الثالث، للفصل الخامس - تكوين الخدمات الجزء ١

١. تكوين SSH للسماح بتسجيل الدخول الجذر باستخدام كلمة المرور (تلميح: PermitrootLogin).

٢. ابدأ تشغيل خدمة SSH واتصل بها من النظام المضيف كمستخدم root.

٣. تكوين خدمة SSH للبدء في وقت الإقلاع.

٤. قم بتغيير كلمة مرور الجذر وقم بإنشاء مفاتيح مضيف SSH جديدة.

٥. النينجا! اجعل نسخة Kali الخاصة بك نقطة وصول عن طريق تثبيت **hostapd** وبدء تشغيله في وقت الإقلاع. قم بذلك بتكوين خدمة نظام مخصص! *هذا الجزء من التمرين قيد الاختبار*

الإجابة:

١. عين **PermitrootLogin** لـ **yes** في /etc/ssh/sshd_config

٢. ابدء sshd:

systemctl start ssh

٣. تمكين sshd عند الإقلاع:

systemctl enable ssh

٤. لأسباب أمنية، قم بتغيير كلمة مرور الجذر وقم بإنشاء مفاتيح مضيف SSH جديدة:

```
root@kali:~# passwd
[...]
root@kali:~# rm /etc/ssh/ssh_host_*
root@kali:~# dpkg-reconfigure openssh-server
root@kali:~# service ssh restart
```

٥. النينجا فقط! hostapd (برنامج نقطة الوصول للمضيف) هو نقطة وصول لبرامج مساحة المستخدم قادرة على تحويل بطاقات واجهة الشبكة العادية إلى نقاط وصول وخوادم مصادقة. لتهيئة خدمة hostapd يدويًا من خلال systemd:

ثبيت وتكوين المتطلبات الأساسية:

```
apt-get install hostapd
nano /etc/systemd/system/hostapd.service
```

أضف الاختبار التالي لملف hostapd.service:

```
[Unit]
Description=Hostapd WPE Service
After=network.target

[Service]
Type=simple
User=root
ExecStart=/usr/sbin/hostapd /etc/hostapd/hostapd.conf
Restart=on-abort

[Install]
WantedBy=multi-user.target
```

- قم بإنشاء أو نسخ ملف hostapd.conf إلى /etc/hostapd/hostapd.conf
- تعطيل مدير الشبكة! أعد تشغيل الخدمة وتمكينها في وقت الإقلاع. تأكد من أن hostapd يعمل بالفعل عند بدء الخدمة.

```
systemctl stop NetworkManager.service
systemctl disable NetworkManager.service
sudo nmcli radio wifi off
sudo rfkill unblock wlan
systemctl enable hostapd
systemctl start hostapd
ps -ef |grep hostapd
systemctl status hostapd
systemctl stop hostapd
ps -ef |grep hostapd
```

ملاحظة: إذا كنت تعمل على جهاز افتراضي، أو كنت تستخدم بطاقة Atheros، فقد تواجه مشكلات ("EEPROM magic" أو فشل البرامج الثابتة، وما إلى ذلك) مع المحول اللاسلكي المستند إلى USB. إذا كانت هذه هي الحالة، أخرج "eject" المحول في إعدادات VM الخاصة بك، افصله، أغلق VM بشكل سليم. أدخل البطاقة وقم بتشغيل الجهاز الافتراضي. إذا لم ينجح أي من هذا، فلا تقلق. هذا أمر صعب للغاية خاصة بسبب VM.

ملاحظة: **systemctl status hostapd** هو pal استكشاف الأخطاء وإصلاحها.

التمرين الرابع، الفصل الخامس - تكوين الخدمات الجزء الثاني

في هذا التمرين، سنقوم بتثبيت masscan. هذه أداة رائعة وسيساعد التثبيت الكامل في مراجعة بعض مفاهيم التكوين التي استكشفناها في هذا الفصل. يتم تقسيم العملية إلى عدة خطوات:

١. قم بتثبيت واباتشي خدمات PostgreSQL.
٢. كوِّن أباتشي و PostgreSQL للبدء في وقت الإقلاع.
٣. قم بتثبيت masscan، وهي متطلبات مسبقة وواجهة ويب ماسكان للأمن الشامل. استخدم حزم Apache / PostgreSQL.

Install masscan, it's prerequisites and Offensive Security's masscan web interface. Use an Apache / PostgreSQL stack.

٤. استيراد فحص سابق واعرض النتائج.
٥. قم بحماية تثبيت Apache باستخدام htaccess اسم مستخدم / كلمة مرور.

الإجابات:

سيكون هذا الحل معطلاً قليلاً. للبدء، راجع نسخة من مستودع masscan-web-ui:

```
root@kali:~# cd /root/
root@kali:~# git clone https://github.com/offensive-security/masscan-web-ui
```

بعد ذلك، تأكد من وجود جميع متطلبات masscan الرئيسية ونسخها عبر ملفات واجهة الويب MASSCAN إلى جذر الويب. لاحظ أنه إذا كنت تقوم بنسخ ولصق سطر **apt-get**، فهذا طويل. تأكد من انتزاع كل شيء:

```
root@kali:~# apt-get install apache2 php libapache2-mod-php php-xml postgresql php-pgsql
mv masscan-web-ui/* /var/www/html/
rm /var/www/html/index.html
```

إبدء تشغيل Apache و Postgres:

```
systemctl start apache2
systemctl start postgresql
```

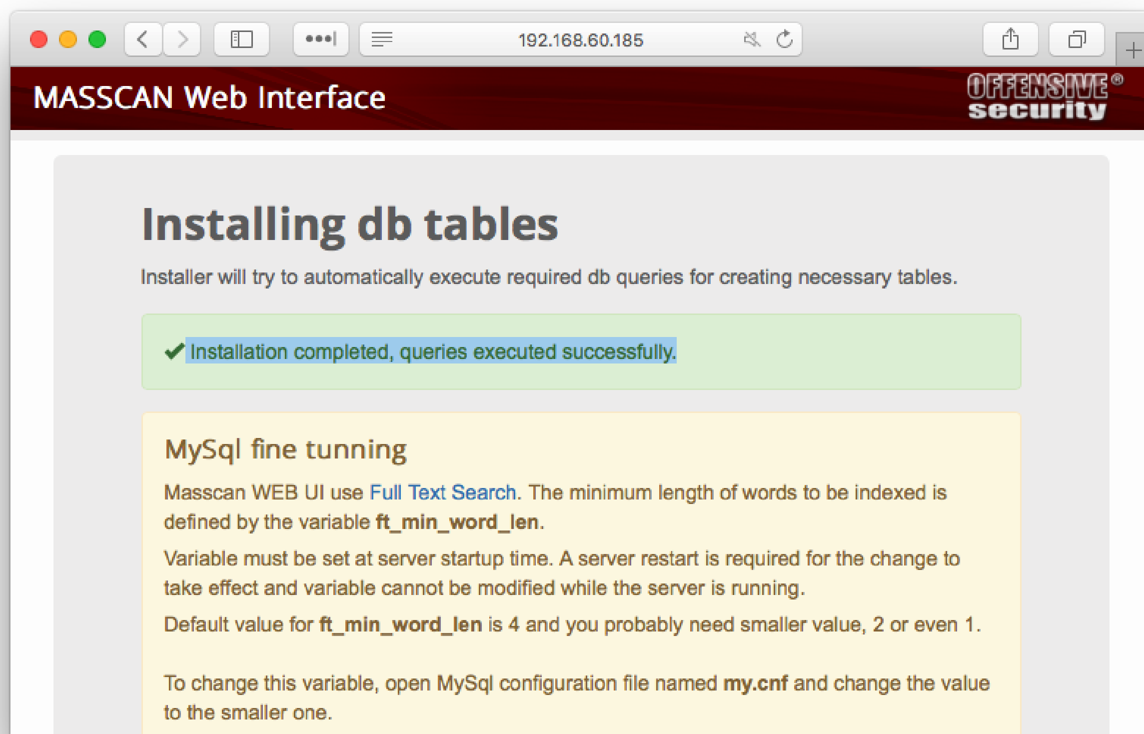
مع بدء Apache و PostgreSQL، تثبيت masscan و index.html الافتراضي من Apache، يمكنك تصفح خادم Apache الخاص بك لرؤية ماسكان. ومع ذلك، فإنه يشكو بحق من فشل مصادقة كلمة المرور. دعنا نصلح ذلك. إنشاء مستخدم ماسكان وإنشاء قاعدة بيانات ماسكان.

```
root@kali:~# su - postgres
postgres@kali:~$ createuser -P masscan
Enter password for new role:
Enter it again:
postgres@kali:~$ createdb -T template0 -E UTF-8 -O
masscan masscandb
exit
```

بعد ذلك، قم بتعديل كلمة المرور التي قمت بتعيينها واسم قاعدة البيانات (masscandb) في أسطر **define**:

```
root@kali:~# nano /var/www/html/config.php
[...]
root@kali:~# grep ^define /var/www/html/config.php
define('DB_DRIVER',        'pgsql');
define('DB_HOST',      '127.0.0.1');
define('DB_USERNAME',  'masscan');
define('DB_PASSWORD',  'toortoor');
define('DB_DATABASE',  'masscandb');
```

تصفح http://localhost على جهازك المحلي (أو العنوان البعيد إذا كنت تتصفح من خارج الجهاز الإفتراضي) والذي يجب أن يشير إلى أنه تم إعداد ماسكان بشكل صحيح:



بعد ذلك، دعنا نستورد بعض نتائج الفحص من فحص تم تشغيله مسبقًا. سنقوم بمسح قاعدة البيانات لأن هذه هي المرة الأولى التي نستخدم فيها ماسكان:

```
root@kali:~# wget https://kali.training/downloads/masscan.xml
root@kali:~# php /var/www/html/import.php /root/masscan.xml
Do you want to clear the database before importing (yes/no)?: yes

Clearing the db
Reading file
Parsing file
```

```
Processing data (This may take some time depending on file size)

Summary:
Total records:4646
Inserted records:4646
Took about:10 seconds
root@kali:~#
```

بعد ذلك، تصفح http://localhost لعرض البيانات المستوردة. نظرًا لأن هذه "بيانات حساسة"، فإننا نريد حماية مجلد الويب الجذر بكلمة مرور. للقيام بذلك، يجب أن نبدأ بتوجيهات Apache:

```
root@kali:~# nano /etc/apache2/sites-enabled/000-default.conf
```

أضف هذه الأسطر:

```
AuthType Basic
AuthName "Restricted Content"
AuthUserFile /etc/apache2/htpasswd
Require valid-user
```

ودعنا ننشئ بيانات اعتماد لمستخدم جديد:

```
root@kali:~# htpasswd -c /etc/apache2/htpasswd myuser
```

أخيرًا، استعرض تصفح http://localhost، وأدخل بيانات اعتمادك واعرض التقرير.

هل تعلم؟

هل تتذكر سياسة Kali Linux لتعطيل خدمات الشبكة افتراضياً؟ تم تكوين هـذه السيـاسة من

/lib/systemd/system-preset/{95-kali.preset،99-default.preset}

نقطة وصول راسبيري باي

إذا لم يكن لديك Raspberry Pi 3، فعليك الحصول على واحدة. فهي رائعة للغاية وغير مكلفة نسبيًا. في هذا التمرين، ستقوم بتكوين Raspberry Pi 3 ليتم تشغيله كنقطة وصول لاسلكية، مما يمنح المستخدمين المتصلين إمكانية الوصول إلى الإنترنت. هذا التمرين رائع لأنك ستقوم بتثبيت Kali على Raspberry Pi وتعديل الملفات وتغيير أذونات الملفات وتكوين واجهات الشبكة وتثبيت الخدمات وتكوينها وتكوين قواعد iptables والمزيد. إنها نظرة عامة رائعة.

إليك ما عليك القيام به:

١. قم بتثبيت Kali على Raspberry Pi 3. يمكنك استخدام صورة مخصصة، ولكن إذا قمت بذلك، فقد يكون لديك المزيد من استكشاف الأخطاء وإصلاحها. إذا لم تكن متأكدًا، فاستخدم صورة المخزون التي تمت كتابة هذا الحل من أجلها.

٢. تطبيق أمان WPA2 على AP.

٣. قم بتكوين **eth0** على أنه DHCP، و**wlan0** على أنه ثابت.

٤. قم بتكوين Raspberry Pi كخادم DHCP لأي عميل لاسلكي وتعيين مصادقة بـ DHCP لمدة ١٢ ساعة.

٥. اجعل خادم SSH يبدأ في وقت الإقلاع حتى تمكن SSH إلى Raspberry Pi بمجرد تشغيله.

٦. إعادة توجيه كل حركة المرور الصادرة، بما في ذلك DNS، من **wlan0** إلى **eth0**.

٧. السماح بالاتصالات الداخلية (ذات الحالة) الواردة من **eth0** إلى **wlan0**.

٨. تلميح: على الرغم من أنك لم نتعلم عن **hostapd** أو **dnsmasq**، إلا أنك ستستخدمها في هذا التمرين.

٩. الغش الجزئي: على الرغم من أن هذا المقال لم يكتب لكالي (ولن يعمل كما هو مكتوب في كالي)، إلا أنه مصدر إلهام لهذا التمرين، ويستحق المراجعة. بفضل فيل مارتن للإلهام.

الإجابات:

سيتطلب هذا بعض الأشياء:

- ❖ Raspberry Pi 3: يمكنك استخدام طراز أقدم بشبكة wifi USB ولكنك لوحدك عندما يتعلق الأمر بتكوين **wlan0**.
- ❖ hostapd: يؤدي هذا إلى إنشاء نقطة اتصال.
- ❖ dnsmasq: يقوم هذا بإعادة توجيه DNS ويوفر قطع DHCP.
- ❖ dhcpcd5: عميل DHCP (الذي يقوم أيضًا بأشياء أخرى رائعة لإدارة الشبكة).

احصل على الحزم المطلوبة:

```
apt-get install dnsmasq hostapd dhcpcd5
```

أولاً، دعنا نطلب من dhcpcd تجاهل إعداد wlan0. سنقوم بتكوين عنوان IP ثابت لاحقًا:

```
nano /etc/dhcpcd.conf
```

ضع هذا فوق أي سطور واجهة قد تكون في الملف:

```
denyinterfaces wlan0
```

الآن، فلنقم بإعداد واجهة wifi الخاصة بنا. إذا كان لديك Pi 2 مع محول USB wi-fi، فتابع وقم بتوصيله الآن. تحرير ملف الواجهات:

```
nano /etc/network/interfaces
```

وأضف هذا القسم:

```
allow-hotplug wlan0

iface wlan0 inet static

    address 172.24.1.1

    netmask 255.255.255.0
```

network 172.24.1.0

broadcast 172.24.1.255

أعد تشغيل dhcpcd باستخدام:

```
root@kali:~# service dhcpcd restart
```

ثم أعد تحميل تكوين wlan0 باستخدام:

```
root@kali:~# ifdown wlan0; ifup wlan0
```

بعد ذلك، فلنقم بتكوين hostapd بملف تكوين جديد. لاحظ أنه تم تكوين SSID وكلمة المرور لنقطة الوصول الخاصة بك.

```
root@kali:~# nano /etc/hostapd/hostapd.conf
[..]
root@kali:~# cat /etc/hostapd/hostapd.conf

# This is the name of the WiFi interface we configured above
interface=wlan0

# Use the nl80211 driver with the brcmfmac driver
driver=nl80211

# This is the name of the network
```

```
ssid=Kali-Pi3

# Use the 2.4GHz band
hw_mode=g

# Use channel 6
channel=6

# Enable 802.11n
ieee80211n=1

# Enable WMM
wmm_enabled=1

# Enable 40MHz channels with 20ns guard interval
ht_capab=[HT40][SHORT-GI-20][DSSS_CCK-40]

# Accept all MAC addresses
macaddr_acl=0

# Use WPA authentication
auth_algs=1

# Require clients to know the network name
ignore_broadcast_ssid=0

# Use WPA2
```

```
wpa=2

# Use a pre-shared key
wpa_key_mgmt=WPA-PSK

# The network passphrase
wpa_passphrase=raspberrytoor

# Use AES, instead of TKIP
rsn_pairwise=CCMP
```

عند هذه النقطة، يمكننا اختبار الأشياء. شغل:

```
root@kali:~# /usr/sbin/hostapd /etc/hostapd/hostapd.conf
```

هذا يدل على تشغيل ناجح. لاحظ أن الأخطاء المتعلقة بوضع المراقبة ليست ذات صلة بنا. بالنسبة إلى RPi3 باستخدام برنامج nexmon، نحتاج (أو تطبيق) الـ *nexutil -m2*.

```
root@kali:~# /usr/sbin/hostapd /etc/hostapd/hostapd.conf
Configuration file: /etc/hostapd/hostapd.conf
Failed to create interface mon.wlan0: -95 (Operation not supported)
wlan0: Could not connect to kernel driver
Using interface wlan0 with hwaddr b6:ae:d7:42:a1:70 and ssid "Kali-Pi3"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
```

يمكنك الاتصال بنقطة الوصول هذه وسيعرض hostapd بعض الإخراج:

wlan0: STA 78:4f:43:7c:6d:32 IEEE 802.11: associated

وبمجرد إدخال كلمة المرور، سترى شيئًا مثل هذا:

wlan0: AP-STA-CONNECTED 78:4f:43:7c:6d:32

wlan0: STA 78:4f:43:7c:6d:32 RADIUS: starting accounting session 5991CC2F-00000000

wlan0: STA 78:4f:43:7c:6d:32 WPA: pairwise key handshake completed (RSN)

wlan0: STA 78:4f:43:7c:6d:32 IEEE 802.11: disassociated

wlan0: AP-STA-DISCONNECTED 78:4f:43:7c:6d:32

wlan0: INTERFACE-DISABLED

wlan0: STA 00:00:00:00:00:00 IEEE 802.11: disassociated

wlan0: INTERFACE-ENABLED

wlan0: STA 78:4f:43:7c:6d:32 IEEE 802.11: associated

لاحظ أن عميلك ربما ينقطع الاتصال به ويعاد الاتصال لأنه لم يحصل على عنوان IP. هذا امر طبيعي. لن تحصل على عنوان IP حتى نقوم بتكوين dnsmasq. استمتع بهذا! يمنحك فكرة عن كيفية عمل هذه العملية، خلف الكواليس.

اضغط على Ctrl-C لإيقاف **hostapd**.

بعد ذلك، سنخبر hostapd بمكان العثور على ملف التكوين الخاص به:

```
root@kali:~# nano /etc/default/hostapd
```

ابحث عن سطر ""=DAEMON_CONF# واستبدله بـ:

DAEMON_CONF="/etc/hostapd/hostapd.conf"

لنقم بتعديل **dnsmasq**:

```
root@kali:~# mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
root@kali:~# nano /etc/dnsmasq.conf
```

يجب أن يبدو كالتالي:

```
interface=wlan0       # Use interface wlan0
listen-address=172.24.1.1 # Set our listening address
bind-interfaces      # Bind to the interface to make sure we aren't sending things elsewhere
server=8.8.8.8       # Forward DNS requests to Google DNS
domain-needed        # Don't forward short names
bogus-priv           # Never forward addresses in the non-routed address spaces.
dhcp-range=172.24.1.50,172.24.1.150,12h   #   Assign   IP addresses between 172.24.1.50 and 172.24.1.150 with a 12 hour lease time
```

الأن لدينا واجهتان نشطتان، وعندنا عميل DHCP لـ الروسفيري الخاص بنا وخادم DHCP لمضيفي الوايرليس الخاص بنا. الأن نحتاج لإعادة توجيه حركة المرور بين واجهات wifi و ethernet. يمكننا تحقيق ذلك على الفور باستخدام أمر بسيط لتحديث proc/:

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
```

ومع ذلك، لن يلتزم هذا التغيير بين عمليات إعادة التشغيل. نحن بحاجة إلى جعلها دائمة من خلال sysctl:

```
root@kali:~# nano /etc/sysctl.conf
```

إلغي تعليق السطر الذي يحتوي على **net.ipv4.ip_forward =1**:

```
root@kali:/var/www/html# grep ip_forward /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

إن عملية إعادة التوجيه ليست كافية تمامًا لمنح مضيفي wifi الخاصين بنا إمكانية الوصول إلى الإنترنت (من خلال واجهة eth0). نحن بحاجة إلى iptables لمساعدتنا على القيام بذلك.

```
root@kali:~# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
root@kali:~# iptables -A FORWARD -i eth0 -o wlan0 \
> -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
root@kali:~# iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

دعونا نبسط هذه الأوامر:

١. عندما يتم العثور على اتصال جديد (`-t nat`)، نريد تبديل -alter- الحزم لأنها على وشك الخروج (A POSTROUTING-) على واجهة إيثرنت (o eth0-). الهدف j- MASQUERADE يحجب عنوان IP الخاص للعميل بعنوان IP الخارجي لجدار الحماية / البوابة (Kali Pi).

٢. بعد ذلك، نلحق (A-) بقاعدة إلى سلسلة FORWARD (يتم توجيه الحزم عبر Pi) والتي تقبل (j ACCEPT-) الحزم من eth0 إلى wlan0 (i eth0 –o wlan0-) التي تنتمي إلى (ESTABLISHED) أو المتعلقة (RELATED) باتصال موجود.

٣. أخيرًا، سنعيد توجيه -forward - (ونقبل -accept-) جميع الحزم من wlan0 إلى eth0.

تحقق من قواعدنا:

```
root@kali:~# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

إخراج قواعدنا إلى ملف:

```
iptables-save > /etc/iptables.ipv4.nat
```

قم بتطبيق هذه القواعد في كل مرة نقوم فيها بتشغيل Pi عن طريق تحرير ملف **/etc/rc.local**:

```
root@kali:~# nano /etc/rc.local
[...]
root@kali:~# more /etc/rc.local
#!/bin/sh -e
iptables-restore < /etc/iptables.ipv4.nat
```

اجعل الملف قابلاً للتنفيذ:

```
root@kali:~# chmod 711 /etc/rc.local
root@kali:~# ls -l /etc/rc.local
-rwx--x--x 1 root root 57 Aug 10 19:37 /etc/rc.local
```

كما رأينا، يتم شحن **hostapd** و **dnsmasq** مع جميع مزايا نظام التهيئة *-init system-* (انظر /etc/init.d)، لذلك دعونا نبدأ الخدمات ونتحقق منها:

```
root@kali:~# systemctl start hostapd dnsmasq
root@kali:~# systemctl status hostapd dnsmasq
● hostapd.service - LSB: Advanced IEEE 802.11 management daemon
   Loaded: loaded (/etc/init.d/hostapd; generated; vendor preset: disabled)
   Active: active (running) since Mon 2017-08-14 19:24:43 UTC; 2s ago
```

```
[...]

● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server

   Loaded: loaded (/lib/systemd/system/dnsmasq.service; disabled; vendor preset:

   Active: active (running) since Mon 2017-08-14 19:24:43 UTC; 2s ago
```

ولتمكنها للعمل بعد إعادة الإقلاع:

```
root@kali:~# systemctl enable hostapd dnsmasq

hostapd.service is not a native service, redirecting to systemd-sysv-install.

Executing: /lib/systemd/systemd-sysv-install enable hostapd

Synchronizing state of dnsmasq.service with SysV service script with /lib/systemd/systemd-sysv-install.

Executing: /lib/systemd/systemd-sysv-install enable dnsmasq
```

أخيرًا، أعد التشغيل وتأكد من الالتزام بالقواعد بعد إعادة التشغيل. بمجرد إعادة التشغيل، يجب أن تكون قادرًا على الاتصال بـ "Kali Pi" والتصفح!

تمرين الشهادة للفصل الخامس

١. بأي أداة يمكنك التحكم في الشبكة في الواجهة الرسومية لـ gnome؟

- ifupdown
- systemctl
- NetworkManager
- /etc/network/interfaces

٢. يعد ملف الواجهات جزءًا مهمًا من تكوين الشبكة بسطر الأوامر. ما هو المجلد الخاص بها؟

- /etc/networks
- /etc/init.d
- /etc/network
- /etc/init

٣. ما هو اسم حزمة سطر الأوامر المستخدمة عادة في كالي لتكوين الشبكة من سطر الأوامر؟

- systemctl
- init.d
- ifupdown
- hosts

٤. عند تكوين شبكة من سطر الأوامر (على سبيل المثال مع ifup أو ifdown) أي سطر سيبدأ القسم لتكوين شبكة يدوي؟

```
o iface eth0 inet auto
o iface eth0 inet auto
o iface eth0 inet auto
o iface eth0 inet static
```

٥. ما هي الأساليب التي يمكن استخدامها لتكوين أجهزة الشبكة في Kali Linux؟ اختر كل ما يمكن تطبيقه:

- رسوميا باستخدام NetworkManager
- بسطر الأوامر باستخدام ملفات network. في المجلد /etc/system/network
- بسطر الأوامر بواسطة ملف /etc/network/interfaces
- بسطر الأوامر بواسطة systemd-networkd
- بسطر الأوامر باستخدام ifupdown

٦. أي ملف يحتوي على كلمات مرور المستخدم المشفرة؟

- /etc/group
- /etc/shadow
- /etc/passwd
- لاشيء مما سبق

٧. ما هو الأمر المستخدم لإضافة مستخدمين؟

- o passwd -l
- o adduser
- o chuser
- o useradd

٨. ما هو الأمر الذي سيعلق حساب المستخدم؟

- o **useradd -s** *olduser*
- o **passwd -l** *olduser*
- o **passwd -s** *olduser*
- o **rmuser -l** *olduser*

٩. ما هو الصحيح لخدمة SSH على تثبيت كالي الافتراضي؟ اختر كل ما ينطبق.

☐ يتم إنشاء المفاتيح الإفتراضية من صورة مباشرة مسبقا

☐ يحظر التكوين الافتراضي عمليات تسجيل الدخول المستندة إلى كلمة المرور

☐ يحظر ملف التكوين الافتراضي عمليات تسجيل الدخول المستندة إلى الشهادات

☐ تم تعطيل خدمة SSH بشكل افتراضي

☐ يتم تثبيت خدمة SSH بشكل افتراضي

١٠. ما هو الأمر الشائع استخدامه لبدء تشغيل خدمات مثل ssh و postgresql؟

- o service
- o systemctl
- o init
- o run

١١. ما هو الأمر المستخدم لإضافة قاعدة بيانات postgresql جديدة؟

- o dropdb
- o createdb
- o psql -n
- o db_create

١٢. أي من هذه الأوامر ليس من أوامر postgresql؟

- o createuser
- o pg_createuser
- o psql
- o createdb

١٣. أي من هذه الأوامر تنشئ قاعدة بيانات postgres باسم db_new؟

- o psql -h localhost -c db_new -O dbuser dbuser
- o createdb -T template0 -E UTF-8 -O dbuser db_new
- o pg_create -o dbuser -n db_new -E UTF-8
- o createdb -T template0 -E UTF-8 -n db_new

١٤. أي مما يلي ليس لها علاقة بـ Apache2؟ اختر واحدة.

- o a2enmod
- o systemctl start apache
- o /etc/apache2
- o /var/www/html

١٥.   أي مما يلي ليس له علاقة بـ Apache2؟

- /etc/apache2/mods-available
- /etc/apache2/ports.conf
- DocumentRoot
- htpasswd
- .htaccess
- Apachectl

١٦.   في كالي، ما هو المسؤول عن تسلسل الإقلاع، ولكنه يعمل أيضًا بصفة دائمة كمدير خدمة كامل الميزات وبدء الخدمات ومراقبتها؟

- init.d
- systemd
- grub
- systemctl

١٧.   أي أمر سيفحص الوضع الحالي لخدمة postgresql؟

```
o /etc/init/postgresql status
o ps | grep postgresql
o sudo status postgresql
o systemctl status postgresql
```

الإجابات الصحيحة:

1. NetworkManager
2. /etc/network
3. ifupdown
4. iface eth0 inet static
5. On the command line with .network files in the /etc/systemd/network directory

   On the command line with ifupdown

   On the command line via the /etc/network/interfaces file

   Graphically with NetworkManager

   On the command line with systemd-networkd
6. /etc/shadow
7. **adduser**
8. **passwd -l** *olduser*
9. The SSH service is installed by default

   The default configuration blocks password-based logins

   The SSH service is disabled by default

   The default keys from a live image are pre-generated
10. **systemctl**
11. **createdb**
12. pg_createuser
13. **createdb -T template0 -E UTF-8 -O dbuser db_new**
14. **systemctl start apache**
15. apachectl
16. systemd
17. **systemctl status postgresql**

#usermod -a -G group user

---((الفصل السادس))---

٦. الحصول على المساعدة

بغض النظر عن عدد سنوات الخبرة التي لديك، فلا شك في أنك ستواجه مشكلة - عاجلاً أم آجلاً. غالبًا ما يكون حل هذه المشكلة مسألة فهمها ثم الاستفادة من الموارد المختلفة لإيجاد حل أو حل بديل.

في هذا الفصل، سنناقش مصادر المعلومات المختلفة المتاحة ونناقش أفضل الاستراتيجيات للعثور على المساعدة التي تحتاجها أو حل المشكلة التي قد تواجهها. سنأخذك أيضًا في جولة في بعض موارد مجتمع Kali Linux المتاحة، بما في ذلك منتديات الويب وقناة Internet Relay Chat (IRC). أخيرًا، سنقدم لك تقريرًا عن الأخطاء وسنوضح لك كيفية الاستفادة من أنظمة حفظ الأخطاء لاستكشاف المشكلات وإصلاحها ووضع استراتيجيات لمساعدتك في تقديم تقرير الأخطاء الخاص بك بحيث يمكن معالجة المشكلات غير الموثقة بسرعة وفعالية.

١.٦. مصادر التوثيق

قبل أن تتمكن من فهم ما يحدث حقًا عند وجود مشكلة، تحتاج إلى معرفة الدور النظري الذي يلعبه كل برنامج مشارك في المشكلة. واحدة من أفضل الطرق للقيام بذلك هي مراجعة وثائق البرنامج. دعنا نبدأ بمناقشة مكان، بالضبط، يمكنك العثور على وثائق لأنها غالبًا ما تكون مبعثرة.

كيفية تجنب إجابات RTFM

يشير هذا الاختصار إلى "Read The F***ing Manual"، ولكن يمكن أيضًا توسيعه بصيغة أكثر ودية، "Read The Fine Manual". تُستخدم هذه العبارة أحيانًا في ردود على أسئلة مبتدئين. إنه أمر مفاجئ إلى حد ما، وينم عن إزعاج معين في سؤال يطرحه شخص لم يكلف نفسه عناء قراءة الوثائق. يقول البعض أن هذه الاستجابة أفضل من عدم الاستجابة على الإطلاق لأن هذا على الأقل يشير إلى أن الإجابة في الوثائق.

عندما تنشر أسئلة، لا تشعر بالضرورة بالإهانة من رد RTFM، ولكن افعل ما بوسعك على الأقل لإثبات أنك قد استغرقت بعض الوقت لإجراء بعض البحث قبل نشر السؤال؛ اذكر المصادر التي استشرتها ووصف الخطوات المختلفة التي اتخذتها شخصيًا للعثور على المعلومات. هذا سيقطع شوطًا طويلًا لإظهار أنك لست كسولًا وتسعى حقًا إلى المعرفة. يُعد اتباع إرشادات Eric Raymond's طريقة جيدة لتجنب الأخطاء الأكثر شيوعًا والحصول على إجابات مفيدة.

http://catb.org/~esr/faqs/smart-questions.html

١.١.٦. الصفحات اليدوية

تحتوي الصفحات اليدوية، بالرغم من كونها قصيرة نسبيًا، على قدر كبير من المعلومات الأساسية. لعرض صفحة يدوية، ما عليك سوى كتابة **man**. عادة ما يكون اسم الوثيقة هو نفس اسم الأمر. على سبيل المثال، للتعرف على الخيارات الممكنة للأمر **cp**، يمكنك كتابة **man cp**.

لا تقوم صفحات Man بتوثيق البرامج التي يمكن الوصول إليها من سطر الأوامر فحسب، بل أيضًا ملفات التكوين ومكالمات النظام ووظائف مكتبة C وما إلى ذلك. في بعض الأحيان يمكن أن تتصادم الأسماء. على سبيل المثال، أمر **read** الخاص بالصدفة له نفس اسم استدعاء نظام القراءة **read**. هذا هو سبب تنظيم الصفحات اليدوية في الأقسام المرقمة التالية:

١. الأوامر التي يمكن تنفيذها من سطر الأوامر

٢. مكالمات النظام (الوظائف التي توفرها النواة)

٣. وظائف المكتبة (تقدمها مكتبات النظام)

٤. الأجهزة (على أنظمة شبيهة بنظام يونكس، هذه ملفات خاصة، توضع عادة في مجلد /dev/)

٥. ملفات التكوين

٦. الألعاب

٧. مجموعات وحدات الماكرو والمعايير

٨. أوامر إدارة النظام

٩. روتينات النواة

يمكنك تحديد قسم الصفحة اليدوية الذي تبحث عنه: لعرض وثائق مكالمة نظام read، يمكنك كتابة man 2 read. عندما لا يتم تحديد أي قسم بشكل صريح، سيتم عرض القسم الأول الذي يحتوي على صفحة يدوية بالاسم المطلوب. وبالتالي، **man shadow** يُرجع shadow (5) لأنه لا توجد صفحات يدوية لـ shadow في الأقسام ١-٤.

بالطبع، إذا كنت لا تعرف أسماء الأوامر، فلن يكون الدليل مفيدًا لك كثيرًا. أدخل الأمر **apropos**، الذي يبحث في الصفحات اليدوية (أو بشكل أكثر تحديدًا وصفها القصير) عن أي كلمات رئيسية تقدمها. يقوم الأمر **apropos** بعد ذلك بإرجاع قائمة بالصفحات اليدوية التي يذكر ملخصها الكلمات الرئيسية المطلوبة جنبًا إلى جنب مع الملخص المكون من سطر واحد من الصفحة اليدوية. إذا اخترت كلماتك الرئيسية جيدًا، فستجد اسم الأمر الذي تحتاجه.

مثال ٦.١. إيجاد **cp** بواسطة الأمر **apropos**

```
$ apropos "copy file"
cp (1)             - copy files and directories
cpio (1)           - copy files to and from
archives
gvfs-copy (1)      - Copy files
gvfs-move (1)      - Copy files
hcopy (1)          - copy files from or to an HFS
volume
install (1)        - copy files and set attributes
ntfscp (8)         - copy file to an NTFS volume.
```

تصفح الوثائق باتباع الروابط

تحتوي العديد من الصفحات اليدوية على قسم "انظر أيضًا"، عادةً بالقرب من نهاية المستند، والذي يشير إلى الصفحات اليدوية الأخرى ذات الصلة بالأوامر المماثلة، أو الوثائق الخارجية. يمكنك استخدام هذا القسم للعثور على الوثائق ذات الصلة حتى عندما لا يكون الخيار الأول هو الأمثل.

بالإضافة إلى **man**، يمكنك استخدام **konqueror** (في KDE) و **yelp** (في GNOME) للبحث في صفحات man أيضًا.

٢.١.٦. وثائق المعلومات info

لقد كتب مشروع GNU أدلة لأغلب برامجه بصيغة المعلومات info، هذا هو السبب في أن العديد من الصفحات اليدوية تشير إلى وثائق المعلومات المقابلة. يقدم هذا التنسيق بعض الميزات ولكن البرنامج الافتراضي لعرض هذه المستندات (يسمى أيضًا **info**) أكثر تعقيدًا بعض الشيء. ننصحك باستخدام **pinfo** (من حزمة pinfo) بدلا من ذلك. لتثبيته، ما عليك سوى تشغيل **apt update** متبوعًا بـ **apt install pinfo** (انظر القسم ٢.٢.٢.٨، "تثبيت الحزم باستخدام APT").

تحتوي وثائق المعلومات على هيكل هرمي وإذا قمت باستدعاء **pinfo** بدون معلمات، فسوف تعرض قائمة بالعُقد المتوفرة في المستوى الأول. عادة، تحمل العقد اسم الأوامر المقابلة.

يمكنك استخدام مفاتيح الأسهم للتنقل بين العقد. بدلاً من ذلك، يمكنك أيضًا استخدام متصفح رسومي (وهو أكثر سهولة في الاستخدام) مثل **konqueror** أو **yelp**.

فيما يتعلق بترجمات اللغة، يكون نظام المعلومات دائمًا باللغة الإنجليزية وغير مناسب للترجمة، على عكس صفحات **man**. ومع ذلك، عندما تطلب من برنامج **pinfo** عرض صفحة معلومات غير موجودة، فسوف تعود إلى صفحة *الدليل* بنفس الاسم (إن وجد)، والتي قد تتم ترجمتها.

٣.١.٦. وثائق خاصة بالحزمة

تحتوي كل حزمة على الوثائق الخاصة بها، وحتى أقل البرامج توثيقًا بشكل عام تحتوي على ملف README يحتوي على بعض المعلومات المهمة و/أو المهمة. يتم تثبيت هذه الوثائق في المجلد **/usr/share/doc/***package***/** (حيث يمثل *package* اسم الحزمة). إذا كانت الوثائق كبيرة بشكل خاص، فقد لا يتم تضمينها في الحزمة الرئيسية للبرنامج، ولكن قد يتم إلغاء تحميلها إلى حزمة مخصصة تسمى عادةً *package*-**doc**. توصي الحزمة الرئيسية عمومًا بحزمة التوثيق بحيث يمكنك العثور عليها بسهولة.

يحتوي المجلد **/usr/share/doc/***package***/** على بعض الملفات المقدمة من دبيان، والتي تكمل الوثائق من خلال تحديد خصائص الحزمة أو التحسينات مقارنة بالتثبيت التقليدي للبرنامج. يشير ملف **README.Debian** أيضًا إلى جميع التعديلات التي تم إجراؤها لتتوافق مع سياسة دبيان. يسمح ملف **changelog.Debian.gz** للمستخدم باتباع التعديلات التي أدخلت على الحزمة بمرور الوقت؛ من المفيد جدًا محاولة فهم ما تغير بين نسختين مثبتتين ليس لهما نفس السلوك. أخيرًا، يوجد أحيانًا ملف **NEWS.Debian.gz** يوثق التغييرات الرئيسية في البرنامج التي قد تهم المسؤول بشكل مباشر.

٤.١.٦. مواقع الويب

في كثير من الحالات، يمكنك العثور على مواقع الويب التي يتم استخدامها لتوزيع برامج مجانية ولجمع مجتمع مطوريها ومستخدميها. يتم تحميل هذه المواقع بالمعلومات ذات الصلة في أشكال مختلفة مثل الوثائق الرسمية والأسئلة الشائعة "frequently asked questions"(FAQ) وأرشيفات القوائم البريدية. في معظم الحالات، تعالج أرشيفات الأسئلة الشائعة أو أرشيف القوائم البريدية المشكلات التي واجهتها. أثناء البحث عن المعلومات عبر الإنترنت، من المفيد للغاية إتقان بنية البحث. نصيحة سريعة: حاول قصر البحث على نطاق معين، مثل النطاق المخصص للبرنامج الذي يسبب لك المشاكل. إذا أعاد البحث عددًا كبيرًا جدًا من الصفحات أو إذا لم تتطابق النتائج مع ما تبحث عنه، فيمكنك إضافة الكلمة الرئيسية **kali** أو **debian** للحد من النتائج واستهداف المعلومات ذات الصلة.

من المشلكة للحل

إذا أعاد البرنامج رسالة خطأ محددة للغاية، فأدخلها في محرك بحث (بين علامتي اقتباس مزدوجتين "، للبحث عن العبارة الكاملة، بدلاً من الكلمات الرئيسية الفردية). في معظم الحالات، ستحتوي الروابط الأولى التي تم إرجاعها على الإجابة التي تحتاجها. في حالات أخرى، ستحصل على أخطاء عامة جدًا، مثل "تم رفض الإذن". في هذه الحالة، من الأفضل التحقق من أذونات العناصر المعنية (الملفات، معرف المستخدم، المجموعات، إلخ). باختصار، لا تعتاد دائمًا استخدام محرك بحث لإيجاد حل لمشكلتك. ستجد أنه من السهل جدًا نسيان استخدام الحس السليم.

إذا كنت لا تعرف عنوان موقع البرنامج، فهناك العديد من الوسائل لتحديد موقعه. أولاً، ابحث عن حقل الصفحة الرئيسية "Home page" في المعلومات الوصفية للحزمة (**apt show** *package*). بدلاً من ذلك، قد يحتوي وصف الحزمة على رابط إلى موقع الويب الرسمي للبرنامج.

إذا لم يتم تحديد عنوان URL، فربما يكون مشرف الحزمة قد ضمّن عنوان URL في ملف **/usr/share/doc/***package***/Copyright**. أخيرًا، قد تتمكن من استخدام محرك بحث (مثل Google و DuckDuckGo و Yahoo وما إلى ذلك) للعثور على موقع البرنامج.

٥.١.٦. وثائق كالي في docs.kali.org

يحتفظ مشروع كالي بمجموعة من الوثائق المفيدة على http://docs.kali.org. على الرغم من أن هذا الكتاب يغطي جزءًا كبيرًا مما يجب أن تعرفه عن Kali Linux، فقد لا تزال الوثائق هناك مفيدة لأنها تحتوي على إرشادات خطوة بخطوة (مثل الكثير من الإرشادات) حول العديد من الموضوعات.

http://docs.kali.org/

دعنا نراجع الموضوعات المختلفة التي يتم تناولها هناك:

- ❖ الشروع في العمل: سلسلة من التعليمات، بما في ذلك تعليمات التنزيل، لأولئك الجدد على Kali
- ❖ Kali Linux Live: وثائق تصف كيفية استخدام Kali Linux كنظام مباشر
- ❖ تثبيت Kali Linux: وثائق مختلفة تصف تثبيت Kali Linux، بما في ذلك كيفية تثبيته جنبًا إلى جنب مع أنظمة التشغيل الأخرى
- ❖ Kali Linux على ARM: العديد من الوصفات حول تشغيل Kali Linux على مختلف الأجهزة القائمة على ARM
- ❖ استخدام Kali Linux: العديد من الإرشادات حول العديد من الطلبات الشائعة

- ❖ تخصيص Kali Linux: تعليمات للمتعبين الذين يرغبون في إعادة بناء Kali بناءً على متطلباتهم الخاصة
- ❖ Kali Community Support: يشير إلى المجتمعات المختلفة حيث يمكنك الحصول على الدعم والتوضيحات حول كيفية إرسال تقارير الأخطاء
- ❖ سياسات Kali Linux: توضيحات حول ما يجعل Kali Linux مميزًا عند مقارنته بتوزيعات Linux الأخرى
- ❖ The Kali Linux Dojo: مقاطع فيديو لورشات Black Hat و DEF CON

٢.٦. مجتمعات كالي لينكس

هناك العديد من مجتمعات Kali Linux حول العالم تستخدم العديد من الأدوات المختلفة للتواصل (المنتديات والشبكات الاجتماعية، على سبيل المثال). في هذا القسم، سنقدم فقط مجتمعين رسميين لـ Kali Linux.

١.٢.٦. منتديات الويب على forums.kali.org

توجد منتديات المجتمع الرسمية لمشروع كالي لينكس على forums.kali.org. مثل كل منتدى قائم على الويب، يجب عليك إنشاء حساب لتتمكن من النشر ويتذكر النظام ما هي المنشورات التي رأيتها بالفعل، مما يجعل من السهل متابعة المحادثات على أساس منتظم.

قبل النشر، يجب عليك قراءة قواعد المنتدى:

http://docs.kali.org/community/kali-linux-community-forums

لن نقوم بكتابتها هنا ولكن تجدر الإشارة إلى أنه لا يُسمح لك بالتحدث عن الأنشطة غير القانونية مثل اختراق شبكات الأشخاص الآخرين. يجب أن تكون محترمًا لأعضاء المجتمع الآخرين لإنشاء مجتمع ترحيبي. الإعلان محظور ويجب تجنب المناقشات خارج الموضوع. هناك فئات كافية لتغطية كل شيء تود مناقشته حول Kali Linux.

٦.٢.٢. قناة # kali linux IRC على Freenode

IRC هو نظام دردشة في الوقت الحقيقي. تحدث المناقشات في غرف الدردشة التي تسمى القنوات وعادة ما تتمحور حول موضوع أو مجتمع معين. يستخدم مشروع Kali Linux قناة #kali-linux على شبكة Freenode (يمكنك استخدام chat.freenode.net كخادم IRC، على المنفذ 6667 لاتصال مشفر بـ TLS أو منفذ 6666 لاتصال نص واضح).

للانضمام إلى المناقشات حول IRC، يجب عليك استخدام عميل IRC مثل **hexchat** (في الوضع الرسومي) أو **irssi** (في وضع وحدة التحكم). يتوفر أيضًا عميل قائم على الويب على webchat.freenode.net.

في حين أنه من السهل حقًا الانضمام إلى المحادثة، يجب أن تكون على دراية بأن قنوات IRC لها قواعدها الخاصة وأن هناك عوامل تشغيل للقنوات (يُطلق لقبهم بـ @) يمكنهم فرض القواعد: يمكنهم طردك من القناة (أو حتى منعك إذا استمرت في عصيان القواعد). قناة #kali-linux ليست استثناء. تم توثيق القواعد هنا:

http://docs.kali.org/community/kali-linux-irc-channel

لتلخيص القواعد: يجب أن تكون ودودًا ومتسامحًا ومعقولًا. يجب تجنب المناقشات خارج الموضوع. على وجه الخصوص، يحظر المناقشات حول الأنشطة غير القانونية /الثغرات/البرمجيات المقرصنة، والسياسة، والأديان. ضع في اعتبارك أن عنوان IP الخاص بك سيكون متاحًا للآخرين.

إذا كنت تريد طلب المساعدة، فاتبع التوصيات الواردة في كيفية تجنب إجابات RTFM: قم بإجراء بحثك أولاً وشارك النتائج. عندما يُطلب منك معلومات تكميلية، يرجى تقديمها بدقة (إذا كان عليك تقديم بعض الإخراج المطول، فلا تلصقها في القناة مباشرة، وبدلاً من ذلك استخدم خدمة مثل Pastebin ونشر عنوان URL الخاص بـ Pastebin فقط).

لا تتوقع إجابة فورية. على الرغم من أن IRC هو منصة اتصال في الوقت الفعلي، إلا أن المشاركين يسجلون الدخول من جميع أنحاء العالم، لذلك تختلف المناطق الزمنية وجداول العمل. قد يستغرق الرد على سؤالك بضع دقائق أو ساعات. ومع ذلك، عندما يدرج الآخرون لقبك في الرد، سيتم تمييز لقبك وسوف يخطرك (إشعار) معظم عملاء IRC، لذا اترك عميلك متصلاً وتحلى بالصبر.

```
/*
$ sudo apt install irssi
$ irssi
/connect chat.freenode.net
/join #kali-linux
للمزيد قم بتنزيل الملف:
https://bit.ly/irssi_tool
*/
```

٣.٦. تقديم تقرير خطأ جيد

إذا فشلت كل جهودك لحل المشكلة، فمن المحتمل أن تكون المشكلة بسبب خطأ في البرنامج. في هذه الحالة، ربما أدت المشكلة إلى تقرير خطأ. يمكنك البحث عن تقارير الأخطاء لإيجاد حل لمشكلتك ولكن دعنا نلقي نظرة على إجراء الإبلاغ عن خطأ إلى Kali أو Debian أو مباشرة إلى مطوري البرنامج حتى تفهم العملية إذا كنت بحاجة إلى إرسال تقريرك الخاص.

الهدف من تقرير الخطأ هو توفير معلومات كافية حتى يتمكن مطورو أو مشرفو البرنامج المعيب (المفترض) من إعادة إنتاج المشكلة وتصحيح سلوكها وتطوير حل لها. هذا يعني أن تقرير الخطأ الخاص بك يجب أن يحتوي على معلومات مناسبة ويجب توجيهه إلى الشخص الصحيح أو فريق المشروع. يجب أن يكون التقرير مكتوبًا بشكل جيد وشاملًا، مما يضمن استجابة أسرع.

يختلف الإجراء الدقيق لتقرير الخطأ اعتمادًا على المكان الذي سترسل فيه التقرير (Kali، Debian، upstream developer) ولكن هناك بعض التوصيات العامة التي تنطبق على جميع الحالات. في هذا الفصل سوف نناقش تلك التوصيات.

٦.٣.١. توصيات عامة

دعنا نناقش بعض التوصيات العامة والمبادئ التوجيهية التي ستساعدك على إرسال تقرير خطأ واضح وشامل ويحسن فرص معالجة المطورين من قبل المطورين في الوقت المناسب.

٦.٣.١.١. كيفية التواصل

اكتب تقريرك باللغة الإنجليزية

ما لم تكن تعرف محادثك، فيجب أن تستخدم لغة إنجليزية بسيطة. إذا كنت متحدثًا أصليًا للغة الإنجليزية، فاستخدم جملًا بسيطة وتجنب الإنشاءات التي قد يصعب فهمها للأشخاص ذوي مهارات محدودة في اللغة الإنجليزية. على الرغم من أن معظم المطورين يتمتعون بذكاء كبير، إلا أن ليس لديهم كلًا مهارات قوية في اللغة الإنجليزية. من الأفضل ألا تفترض.

احترم عمل المطورين

تذكر أن معظم مطوري البرمجيات الحرة (بما في ذلك أولئك الذين يقفون وراء Kali Linux) هم خيرين ويقضون وقت فراغهم المحدود للعمل على البرنامج الذي تستخدمه بحرية. يفعل الكثيرون ذلك بدافع الإيثار. وبالتالي، عندما تقدم تقريرًا عن خطأ، كن محترمًا (حتى لو بدا الخطأ كخطأ واضح من المطور) ولا تفترض أنهم مدينون لك بإصلاح. نشكرهم على مساهمتهم بدلاً من ذلك.

إذا كنت تعرف كيفية تعديل البرنامج وإعادة ترجمته، اعرض مساعدة المطورين في اختبار أي تصحيحات يرسلونها إليك. سيظهر لهم ذلك أنك على استعداد لاستثمار وقتك أيضًا.

كن متفاعلًا وجاهزًا لتقديم المزيد من المعلومات

في بعض الحالات، سيرجع المطور إليك بطلبات للحصول على مزيد من المعلومات أو طلبات لمحاولة إعادة إنشاء المشكلة ربما باستخدام خيارات مختلفة أو باستخدام حزمة محدثة. يجب أن تحاول الرد على هذه الاستفسارات في أسرع وقت ممكن. كلما أرسلت ردك بشكل أسرع، زادت فرصة تمكنهم من حلها بسرعة بينما لا يزال التحليل الأولي جديدًا في أذهانهم.

بينما يجب أن تهدف إلى الاستجابة بسرعة، يجب ألا تسير بسرعة كبيرة: يجب أن تكون البيانات المقدمة صحيحة ويجب أن تحتوي على كل ما طلبه المطورون. سيشعرون بالانزعاج إذا اضطروا لطلب شيء ما مرة أخرى.

٢.١.٣.٦. ما يجب وضعه في تقرير الخطأ

تعليمات إعادة إنتاج المشكلة

لكي تتمكن من إعادة إظهار المشكلة، يحتاج المطورون إلى معرفة ما تستخدمه، ومن أين حصلت عليه، وكيف قمت بتثبيته.

يجب عليك تقديم تعليمات دقيقة خطوة بخطوة تصف كيفية إعادة إظهار المشكلة. إذا كنت بحاجة إلى استخدام بعض البيانات لإعادة إظهار المشكلة، فقم بإرفاق الملف المقابل بتقرير الخطأ. حاول التوصل إلى الحد الأدنى من التعليمات اللازمة لإعادة إنتاج الخطأ.

قدم بعض السياق وحدد توقعاتك

اشرح ما كنت تحاول القيام به وكيف توقعت أن يتصرف البرنامج.

في بعض الحالات، يظهر لك الخطأ فقط لأنك كنت تستخدم البرنامج بطريقة لم يتم تصميمه لها.

في بعض الحالات الأخرى، قد يكون السلوك الذي تصفه بأنه خطأ هو السلوك العادي. كن صريحًا بشأن ما كنت تتوقع أن يفعله البرنامج. هذا سيوضح الوضع للمطورين. يمكنهم إما تحسين السلوك أو تحسين التوثيق، لكي يعرفوا على الأقل أن سلوك برنامجهم يربك بعض المستخدمين!

كن دقيقا

قم بتضمين أرقام إصدارات البرنامج التي تستخدمها، ربما مع أرقام إصدارات تبعياتها. عندما تشير إلى شيء قمت بتنزيله، قم بتضمين عنوان URL الكامل الخاص به.

عندما تتلقى رسالة خطأ، اقتبسها تمامًا كما رأيتها. إن أمكن، ضمّن نسخة من إخراج الشاشة أو لقطة شاشة. ضمّن نسخة من أي ملف سجل ذي صلة، مع التأكد من إزالة أي بيانات حساسة أولاً.

اذكر الإصلاحات الممكنة أو الحلول البديلة

قبل تقديم تقرير الخطأ، ربما حاولت حل المشكلة. اشرح ما حاولت القيام به وما النتائج التي تلقيتها. كن واضحًا جدًا بشأن ما هي الحقيقة وما هي مجرد فرضية من جانبك.

إذا أجريت بحثًا عبر الإنترنت ووجدت بعض التفسيرات حول مشكلة مشابهة، فيمكنك ذكرها، لا سيما عندما تجد تقارير أخطاء مشابهة أخرى في أداة تتبع الأخطاء في دبيان أو في أداة تتبع الأخطاء الأولية.

إذا وجدت طريقة لتحقيق النتيجة المرجوة دون تشغيل الخطأ، يرجى توثيق ذلك أيضًا. سيساعد هذا المستخدمين الآخرين الذين تضرروا من نفس المشكلة.

تقارير الأخطاء الطويلة جيدة

تقرير خلل من سطرين غير كاف؛ يتطلب تقديم جميع المعلومات المطلوبة عادةً عدة فقرات (أو أحيانًا صفحات) من النص.

قدم كل المعلومات التي تستطيع. حاول الالتزام بما هو مناسب، ولكن إذا لم تكن متأكدًا، فالكثير أفضل من القليل.

إذا كان تقرير الخطأ الخاص بك طويلًا حقًا، خصص بعض الوقت لتنظيم المحتوى وتقديم ملخص قصير في البداية.

٣.١.٣.٦. نصائح متنوعة

تجنب تقديم تقارير الأخطاء المكررة

في عالم البرمجيات الحرة، جميع أجهزة تتبع الأخطاء عامة. يمكن تصفح المشكلات المفتوحة ولديها ميزة البحث. وبالتالي، قبل تقديم تقرير خطأ جديد، حاول تحديد ما إذا كان شخص آخر قد أبلغ بالفعل عن مشكلتك.

إذا عثرت على تقرير خطأ حالي، اشترك فيه وربما أضف معلومات تكميلية. لا تنشر تعليقات مثل "أنا أيضًا" أو "+١"؛ لأنها لا تنفع بشيء. ولكن يمكنك الإشارة إلى أنك متاح لمزيد من الاختبارات إذا لم يقدم مقدم الطلب الأصلي ذلك.

إذا لم تعثر على أي تقرير عن مشكلتك، فانتقل وأرسلها. إذا تقرير ذي صلة، فتأكد من ذكرها.

تأكد من استخدام أحدث إصدار

إنه لأمر محبط للغاية أن يتلقى المطورون تقارير أخطاء عن المشكلات التي قاموا بحلها بالفعل أو المشكلات التي لا يمكنهم إعادة إنتاجها باستخدام الإصدار الذي يستخدمونه (غالبًا ما يستخدم المطورون أحدث إصدار من منتجهم). حتى عندما يتم الاحتفاظ بالإصدارات القديمة من قبل المطورين، غالبًا ما يقتصر الدعم على إصلاحات الأمان والمشكلات الرئيسية. هل أنت متأكد من أن الخلل الخاص بك هو واحد من هذه الأخطاء؟

لهذا السبب، قبل تقديم تقرير الأخطاء، يجب عليك التأكد من أنك تستخدم أحدث إصدار من النظام والتطبيق الإشكالي وأنه يمكنك إعادة إنتاج المشكلة في هذا الموقف.

إذا كان Kali Linux لا يقدم أحدث إصدار من التطبيق (لا في kali-rolling ولا في kali-bleeding-edge، راجع القسم ٣.٣.١.٨، "مستودع Kali-Bleeding-Edge")، فلديك حلول بديلة: يمكنك تجريبها جرب التثبيت اليدوي لأحدث إصدار في جهاز افتراضي، أو يمكنك مراجعة سجل التغيير ChangeLog (أو سجل تنفيذ Git) لمعرفة أنه لم يكن هناك أي تغيير يمكن أن يحل المشكلة التي تراها (وثم قم بإيداع الخطأ حتى لو لم تجرب أحدث إصدار).

لا تخلط مشكلات متعددة في تقرير خطأ واحد

إرسال تقرير خطأ واحد لكل مشكلة. بهذه الطريقة، لا تصبح المناقشات اللاحقة فوضوية للغاية ويمكن إصلاح كل خطأ وفقًا لجدوله الزمني. إذا لم تفعل ذلك، فإما أن يكون الخطأ الواحد بحاجة إلى إعادة تعيين الغرض منه عدة مرات ولا يمكن إغلاقه إلا بعد إصلاح جميع المشكلات، أو يجب على المطورين تقديم التقارير التكميلية التي كان عليك إنشاؤها في المقام الأول.

٢.٣.٦. مكان تقديم تقرير خطأ

لتتمكن من تحديد مكان إرسال تقرير الخطأ، يجب أن يكون لديك فهم جيد للمشكلة ويجب أن تكون قد حددت أي جزء من البرنامج تكمن فيه المشكلة.

من الناحية المثالية، تتبع المشكلة وصولاً إلى ملف على نظامك ثم يمكنك استخدام **dpkg** لمعرفة الحزمة التي تمتلك هذا الملف ومن أين تأتي هذه الحزمة. لنفترض أنك عثرت على خطأ في تطبيق رسومي. بعد الاطلاع على قائمة العمليات الجارية (مخرجات **ps auxf**)، اكتشفت أن التطبيق بدأ باستخدام الملف التنفيذي **usr/bin/sparta/** القابل للتنفيذ:

```
$ dpkg -S /usr/bin/sparta</code> sparta: /usr/bin/sparta
$ dpkg -s sparta | grep ^Version: Version: 1.0.1+git20150729-0kali1
```

أنت تعلم أن**usr/bin/sparta/** يتم توفيره بواسطة حزمة **sparta**، والتي توجد في الإصدار ١.٠.١ + git20150729-0kali1. تشير حقيقة أن سلسلة الإصدار تحتوي على kali إلى أن الحزمة تأتي من Kali Linux (أو معدلة بواسطة Kali Linux). أي حزمة لا تحتوي على كالي في سلسلة نسختها (أو في اسم الحزمة) تأتي مباشرة من دبيان (اختبار دبيان بشكل عام).

تحقق مرة أخرى قبل إيداع الأخطاء ضد ديبان

> إذا وجدت خطأ في حزمة مستوردة مباشرة من ديبان، فمن الأفضل الإبلاغ عنها وإصلاحها في جانب ديبان. ومع ذلك، قبل القيام بذلك، تأكد من أن المشكلة قابلة للتكرار على نظام ديبان العادي لأن كالي ربما تسبب في المشكلة عن طريق تعديل الحزم أو التبعيات الأخرى.
> أسهل طريقة لتحقيق ذلك هي إعداد جهاز افتراضي يعمل على Debian Testing، يمكنك العثور على تثبيت صورة ISO لـ Debian Testing على موقع Debian Installer:
>
> https://www.debian.org/devel/debian-installer/
>
> إذا تمكنت من تأكيد المشكلة في الجهاز الإفتراضي، فيمكنك إرسال الخطأ إلى ديبان عن طريق تشغيل **reportbug** داخل الجهاز الإفتراضي واتباع التعليمات المقدمة.

يجب توجيه معظم تقارير الأخطاء حول سلوك التطبيقات إلى مشروعات المنبع الخاصة بها إلا عند مواجهة مشكلة في التكامل: في هذه الحالة، يعد الخطأ خطأ في طريقة حزم البرنامج ودمجه في ديبان أو كالي. على سبيل المثال، إذا كان أحد التطبيقات يوفر خيارات وقت الترجمة التي لا تمكّنها الحزمة أو لا يعمل التطبيق بسبب عدم وجود مكتبة (وبالتالي تسليط الضوء على تبعية مفقودة في المعلومات الوصفية للحزمة)، فقد تواجه تكاملًا مشكلة. عندما لا تعرف نوع المشكلة التي تواجهها، فمن الأفضل عادةً تقديم المشكلة على كلا الجانبين والإحالة إليها.

عادة ما يكون تحديد مصدر المشروع والعثور على مكان تقديم تقرير الخطأ أمرًا سهلاً. عليك فقط تصفح موقع المصدر، والذي تمت الإشارة إليه في حقل **Homepage** للبيانات الوصفية للتعبئة:

```
$ dpkg -s sparta | grep ^Homepage:
Homepage: https://github.com/SECFORCE/sparta
```

٦.٣.٣. كيفية تقديم تقرير خطأ

٦.٣.٣.١. تقديم تقرير خطأ في كالي

يستخدم Kali أداة تتبع الأخطاء المستندة إلى الويب على http://bugs.kali.org حيث يمكنك استشارة جميع تقارير الأخطاء بشكل مجهول، ولكن إذا كنت ترغب في التعليق أو تقديم تقرير خطأ جديد، فستحتاج إلى تسجيل حساب.

٦.٣.٣.١.١. الاشتراك في حساب Bug Tracker

للبدء، ما عليك سوى النقر فوق Signup for new account على موقع bug tracker "تتبع الأخطاء"، كما هو موضح في الشكل ٦.١. "الصفحة الرئيسية لتتبع الأخطاء في Kali".

شكل ٦.١. الصفحة الرئيسية لتتبع الأخطاء في Kali

بعد ذلك، قدم اسم مستخدم وعنوان بريد إلكتروني واستجابة لتحدي CAPTCHA. ثم انقر فوق زر **Signup** للمتابعة (الشكل ٢.٦، "صفحة التسجيل").

KALI LINUX
BUG TRACKER

Signup

Username:	NewBugSubmitter	
E-mail:	nbs@email.com	
Enter the code as it is shown in the box on the right.:	ABFF1	A B F F 1

On completion of this form and verification of your answers, you will be sent a confirmation e-mail to the e-mail address you specified.
Using the confirmation e-mail, you will be able to activate your account. If you fail to activate your account within seven days, it will be purged.
You must specify a valid e-mail address in order to receive the account confirmation e-mail.

Signup

[Login] [Lost your password?]

شكل ٢.٦، صفحة التسجيل

إذا نجحت، ستعلمك الصفحة التالية (الشكل ٣.٦، "صفحة تأكيد التسجيل") بأنه تمت معالجة تسجيل الحساب، وسوف يرسل نظام تعقب الأخطاء رسالة بريد إلكتروني للتأكيد من العنوان الذي قدمته. ستحتاج إلى النقر فوق الرابط الموجود في البريد الإلكتروني لتفعيل حسابك.

بمجرد تنشيط حسابك، انقر فوق **Proceed** للمتابعة إلى صفحة تسجيل دخول متعقب الأخطاء.

KALI LINUX
BUG TRACKER

Account registration processed.

Congratulations, you have registered successfully ! You are now being sent a confirmation e-mail to verify your e-mail address. Visiting the link sent to you in this e-mail will activate your account.

You have seven days to complete the account confirmation process; if you fail to do so within this period, the newly-registered account may be purged.

[Proceed]

شكل ٦.٣. صفحة تأكيد التسجيل

٦.٣.٣.١.٢. إنشاء التقرير

لبدء تقريرك، قم بتسجيل الدخول إلى حسابك وانقر على رابط الإبلاغ عن مشكلة على الصفحة المقصودة. سيتم تقديم نموذج مع العديد من الحقول للملئ، كما هو موضح في الشكل ٦.٤. "نموذج للإبلاغ عن خطأ".

Enter Report Details

*Category	[All Projects] Kali Package Bug
Reproducibility	have not tried
Severity	minor
Priority	normal
Product Version	
*Summary	
*Description	
Steps To Reproduce	
Additional Information	
Upload File (Maximum size: 2,097k)	Parcourir... Aucun fichier sélectionné.
View Status	public private
Report Stay	check to report more issues
* required	Submit Report

شكل ٦.٤. نموذج للإبلاغ عن خطأ

فيما يلي قائمة بجميع الحقول في النموذج:

الفئة "Category" (إلزامية)

يصف هذا الحقل فئة الخطأ الذي ترسله. التقارير التي يمكن أن تعزى إلى حزمة معينة يجب أن تودع في فئات Kali Package Bug أو Kali Package Improvement. يجب أن تستخدم التقارير الأخرى فئات الأخطاء العامة أو طلبات الميزات. الفئات المتبقية مخصصة لحالات استخدام محددة: يمكن استخدام ترقية الأداة لإعلام مطوري Kali بتوافر إصدار جديد من برنامج تم حزمه في Kali. يمكن استخدام طلبات الأدوات الجديدة لاقتراح أدوات جديدة للتعبئة ودمجها في توزيعة كالي.

قابلية اعادة الأنتاج "Reproducibility"

يوثق هذا الحقل ما إذا كانت المشكلة قابلة للتكرار بطريقة يمكن التنبؤ بها أو إذا حدثت بشكل عشوائي إلى حد ما.

الشدة والأولوية "Severity and Priority"

من الأفضل ترك هذه الحقول دون تعديل لأنها مخصصة بشكل أساسي للمطورين. يمكنهم استخدامها لفرز قائمة القضايا حسب شدة المشكلة والأولوية التي يجب التعامل معها.

إصدار المنتج "Product Version"

يجب أن يشير هذا الحقل إلى إصدار Kali Linux الذي تقوم بتشغيله (أو الإصدار الأقرب إلى ما تقوم بتشغيله). فكر مرتين قبل الإبلاغ عن مشكلة في إصدار قديم لم يعد مدعومًا.

ملخص "Summary" (إلزامي)

هذا هو في الأساس عنوان تقرير الخطأ الخاص بك وهو أول شيء يراه الناس. تأكد من أنه يبين سبب تقديم التقرير. تجنب الأوصاف العامة مثل "X لا يعمل" واختر بدلاً من ذلك "X فشل مع الخطأ Y تحت الشرط Z".

الوصف "Description" (إلزامي)

هذا هو نص تقريرك. هنا يجب عليك إدخال جميع المعلومات التي جمعتها حول المشكلة التي تواجهها. لا تنس جميع التوصيات الواردة في القسم السابق.

خطوات إعادة الإنتاج "Steps to Reproduce"

في هذا الحقل، اذكر جميع التعليمات التفصيلية التي تشرح كيفية إثارة المشكلة.

معلومة إضافية "Additional Information"

في هذا القسم، يمكنك تقديم أي معلومات إضافية تعتقد أنها ذات صلة بالمشكلة. إذا كان لديك إصلاح أو حل بديل للمشكلة، فالرجاء تقديمها في هذا القسم.

رفع ملف "Upload File "

لا يمكن تفسير كل شيء بنص عادي. يتيح لك هذا الحقل إرفاق ملفات عشوائية بتقاريرك: لقطات شاشة لإظهار الخطأ، ونماذج المستندات التي تسبب المشكلة، وملفات السجل، وما إلى ذلك.

عرض الحالة "View Status "

اترك هذا الحقل معيناً على "عام" حتى يتمكن الجميع من مشاهدة تقرير الخطأ. استخدم "خاص" فقط للتقارير المتعلقة بالأمان التي تحتوي على معلومات حول الثغرات الأمنية غير المكشوف عنها.

٢.٣.٣.٦. تقديم تقرير خطأ في دبيان

يستخدم دبيان (في الغالب) نظام تتبع الأخطاء المستند إلى البريد الإلكتروني المعروف باسم Debbugs. لفتح تقرير خطأ جديد، سوف ترسل بريدًا إلكترونيًا (مع بنية خاصة) إلى **Submit@bugs.debian.org**. سيؤدي ذلك إلى تخصيص رقم الخطأ XXXXXX وإبلاغك أنه يمكنك إرسال معلومات إضافية عن طريق إرسال **XXXXXX@bugs.debian.org**. يرتبط كل خطأ بحزمة دبيان. يمكنك تصفح جميع أخطاء حزمة معينة (بما في ذلك الخطأ الذي تفكر في الإبلاغ عنه) على **https://bugs.debian.org/package**. يمكنك التحقق من تاريخ خطأ معين على **https://bugs.debian.org/XXXXXX**.

٦.٣.٣.٢.١. إعداد reportbug

بينما يمكنك فتح خطأ جديد باستخدام بريد إلكتروني بسيط، نوصي باستخدام **reportbug** لأنه سيساعدك في صياغة تقرير خطأ قوي يحتوي على جميع المعلومات المطلوبة. من الناحية المثالية، يجب تشغيلها من نظام دبيان (على سبيل المثال، في الجهاز الافتراضي حيث قمت بإعادة إظهار المشكلة).

يبدأ التشغيل الأول لـ **`reportbug`** برنامجًا نصيًا للتكوين. أولاً، حدد مستوى المهارة. يجب عليك اختيار مبتدئ أو قياسي؛ نستخدم هذا الأخير لأنه يوفر تحكمًا أكثر دقة. بعد ذلك، حدد واجهة وأدخل تفاصيلك الشخصية. أخيرًا، حدد واجهة مستخدم. سيسمح لك البرنامج النصي للتهيئة باستخدام وكيل نقل بريد محلي، أو خادم SMTP، أو كخادم أخير، خادم Debian SMTP.

```
Welcome to reportbug! Since it looks like this is the first time you
have

used reportbug, we are configuring its behavior. These settings will
be

saved to the file "/root/.reportbugrc", which you will be free to
edit

further.

Please choose the default operating mode for reportbug.


1 novice    Offer simple prompts, bypassing technical questions.


2 standard  Offer more extensive prompts, including asking about
things
```

```
            that a moderately sophisticated user would be expected to
            know about Debian.

3 advanced  Like standard, but assumes you know a bit more about Debian,
            including "incoming".

4 expert    Bypass most handholding measures and preliminary triage
            routines. This mode should not be used by people unfamiliar
            with Debian's policies and operating procedures.

Select mode: [novice] standard
Please choose the default interface for reportbug.

1 text   A text-oriented console user interface

2 gtk2   A graphical (GTK+) user interface.

3 urwid  A menu-based console user interface

Select interface: text
Will reportbug often have direct Internet access? (You should answer
yes to this question unless you know what you are doing and plan to
check whether duplicate reports have been filed via some other channel.)
[Y|n|q|?]? Y
What real name should be used for sending bug reports?
[root]> Raphaël Hertzog
Which of your email addresses should be used when sending bug reports?
(Note that this address will be visible in the bug tracking system, so you
```

may want to use a webmail address or another address with good spam filtering capabilities.)

[root@localhost.localdomain]> buxy@kali.org

Do you have a "mail transport agent" (MTA) like Exim, Postfix or SSMTP

configured on this computer to send mail to the Internet? [y|N|q|?]? N

Please enter the name of your SMTP host. Usually it's called something

like "mail.example.org" or "smtp.example.org". If you need to use a

different port than default, use the : alternative

format. Just press ENTER if you don't have one or don't know, and so a

Debian SMTP host will be used.

>

Please enter the name of your proxy server. It should only use this

parameter if you are behind a firewall. The PROXY argument should be

formatted as a valid HTTP URL, including (if necessary) a port number; for

example, http://192.168.1.1:3128/. Just press ENTER if you don't have one

or don't know.

>

Default preferences file written. To reconfigure, re-run reportbug with

the "--configure" option.

٢.٢.٣.٣.٦. باستخدام reportbug

بعد اكتمال مرحلة الإعداد، يمكن أن يبدأ تقرير الخطأ الفعلي. ستتم مطالبتك باسم حزمة، على الرغم من أنه يمكنك أيضًا تقديم اسم الحزمة مباشرة على سطر الأوامر بـ **reportbug** *package*).

```
Running 'reportbug' as root is probably insecure! Continue
[y|N|q|?]? y

Please enter the name of the package in which you have
found a problem, or type 'other'

to report a more general problem. If you don't know what
package the bug is in, please

contact debian-user@lists.debian.org for assistance.

> wireshark
```

على عكس النصيحة الواردة أعلاه، إذا كنت لا تعرف أي حزمة بها الخطأ، فيجب عليك الاتصال بمنتدى دعم Kali (الموضح في القسم ٢.٦، "مجتمعات Kali Linux"). في الخطوة التالية، يقوم **reportbug** بتنزيل قائمة الأخطاء التي تم حفظها مقابل الحزمة المحددة ويتيح لك تصفحها لمعرفة ما إذا كان يمكنك العثور عليها.

```
*** Welcome to reportbug.  Use ? for help at prompts. ***

Note: bug reports are publicly archived (including the email address
of

the submitter).

Detected character set: UTF-8

Please change your locale if this is incorrect.

Using '"Raphaël Hertzog" <buxy@kali.org>' as your from address.

Getting status for wireshark...

Verifying package integrity...
```

```
Checking for newer versions at madison...
Will send report to Debian (per lsb_release).
Querying Debian BTS for reports on wireshark (source)...
35 bug reports found:
Bugs with severity important
   1) #478200  tshark: seems to ignore read filters when writing to…
   2) #776206  mergecap: Fails to create output file > 2GB
   3) #780089  wireshark: "On gnome wireshark has not title bar. Does…
Bugs with severity normal
   4) #151017  ethereal: "Protocol Hierarchy Statistics" give misleading…
   5) #275839  doesn't correctly dissect ESMTP pipelining
[...]
  35) #815122  wireshark: add OID 1.3.6.1.4.1.11129.2.4.2
(24-35/35) Is the bug you found listed above [y|N|b|m|r|q|s|f|e|?]? ?
y - Problem already reported; optionally add extra information.
N - (default) Problem not listed above; possibly check more.
b - Open the complete bugs list in a web browser.
m - Get more information about a bug (you can also enter a number
    without selecting "m" first).
r - Redisplay the last bugs shown.
q - I'm bored; quit please.
s - Skip remaining problems; file a new report immediately.
f - Filter bug list using a pattern.
e - Open the report using an e-mail client.
? - Display this help.
(24-35/35) Is the bug you found listed above [y|N|b|m|r|q|s|f|e|?]? n
Maintainer for wireshark is 'Balint Reczey <balint@balintreczey.hu>'.
Looking up dependencies of wireshark...
```

إذا وجدت أن الخطأ الخاص بك قد تم إيداعه بالفعل، فيمكنك اختيار إرسال معلومات تكميلية، وإلا فأنت مدعو لتقديم تقرير خطأ جديد:

```
Briefly describe the problem (max. 100 characters allowed). This
will be

the bug email subject, so keep the summary as concise as possible,
for

example: "fails to send email" or "does not start with -q option

specified" (enter Ctrl+c to exit reportbug without reporting a bug).

> does not dissect protocol foobar

Rewriting subject to 'wireshark: does not dissect protocol foobar'
```

بعد تقديم ملخص من سطر واحد لمشكلتك، يجب عليك تقييم شدتها على مقياس موسع:

How would you rate the severity of this problem or report?

```
1 critical         makes unrelated software on the system (or the whole
                   system) break, or causes serious data loss, or
                   introduces a security hole on systems where you install
                   the package.
2 grave            makes the package in question unusable by most or all
                   users, or causes data loss, or introduces a security
                   hole allowing access to the accounts of users who use
                   the package.
3 serious          is a severe violation of Debian policy (that is, the
                   problem is a violation of a 'must' or 'required'
                   directive); may or may not affect the usability of the
                   package. Note that non-severe policy violations may be
                   'normal,' 'minor,' or 'wishlist' bugs. (Package
                   maintainers may also designate other bugs as 'serious'
and
                   thus release-critical; however, end users should not do
                   so.). For the canonical list of issues worthing a serious
```

```
                    severity you can refer to this webpage:
                    http://release.debian.org/testing/rc_policy.txt
4 important         a bug which has a major effect on the usability of a
                    package, without rendering it completely unusable to
                    everyone.
5 does-not-build    a bug that stops the package from being built from
source.
                    (This is a 'virtual severity'.)
6 normal            a bug that does not undermine the usability of the whole
                    package; for example, a problem with a particular option
                    or menu item.
7 minor             things like spelling mistakes and other minor cosmetic
                    errors that do not affect the core functionality of the
                    package.
8 wishlist          suggestions and requests for new features.

Please select a severity level: [normal]
```

إذا لم تكن متأكدًا، فما عليك سوى الحفاظ على الخطورة الافتراضية للطبيعي "**normal**".

يمكنك أيضًا وضع علامة على تقريرك ببعض الكلمات الرئيسية:

```
Do any of the following apply to this report?

1 d-i         This bug is relevant to the development of debian-installer.
2 ipv6        This bug affects support for Internet Protocol version 6.
3 l10n        This bug reports a localization/internationalization issue.
4 lfs         This bug affects support for large files (over 2 gigabytes).
5 newcomer    This bug has a known solution but the maintainer requests
someone
              else implement it.
6 patch       You are including a patch to fix this problem.
7 upstream    This bug applies to the upstream part of the package.
8 none
```

```
Please select tags: (one at a time) [none]
```

معظم العلامات ليست مقصورة على فئة معينة، ولكن إذا تضمن تقريرك إصلاحًا، فيجب عليك اختيار علامة **patch**.

بمجرد الانتهاء من ذلك، يفتح **reportbug** محرر نص مع قالب يجب عليك تحريره (مثال ٢.٦. "قالب تم إنشاؤه بواسطة **reportbug**"). يحتوي على بعض الأسئلة التي يجب عليك حذفها والإجابة عليها، بالإضافة إلى بعض المعلومات حول نظامك التي تم جمعها تلقائيًا. لاحظ كيفية بناء الأسطر القليلة الأولى. لا يجب تعديلها حيث سيتم تحليلها بواسطة أداة تتبع الأخطاء لتعيين التقرير إلى الحزمة الصحيحة.

مثال ٢.٦. القالب الذي تم إنشاؤه بواسطة `reportbug`

```
Subject: wireshark: does not dissect protocol foobar

Package: wireshark
Version: 2.0.2+ga16e22e-1
Severity: normal

Dear Maintainer,

*** Reporter, please consider answering these questions,
where appropriate ***

   * What led up to the situation?
   * What exactly did you do (or not do) that was effective
(or
```

ineffective)?

* What was the outcome of this action?

* What outcome did you expect instead?

*** End of the template - remove these template lines ***

-- System Information:

Debian Release: stretch/sid

APT prefers testing

APT policy: (500, 'testing')

Architecture: amd64 (x86_64)

Foreign Architectures: i386

Kernel: Linux 4.4.0-1-amd64 (SMP w/4 CPU cores)

Locale: LANG=fr_FR.utf8, LC_CTYPE=fr_FR.utf8 (charmap=UTF-8)

Shell: /bin/sh linked to /bin/dash

Init: systemd (via /run/systemd/system)

Versions of packages wireshark depends on:

ii wireshark-qt 2.0.2+ga16e22e-1

wireshark recommends no packages.

wireshark suggests no packages.

-- no debconf information

بمجرد حفظ التقرير وإغلاق محرر النصوص، يمكنك العودة إلى **reportbug**، الذي يوفر العديد من الخيارات والعروض الأخرى لإرسال التقرير الناتج.

```
Spawning sensible-editor...

Report will be sent to "Debian Bug Tracking System" <submit@bugs.debian.org>

Submit this report on wireshark (e to edit) [Y|n|a|c|e|i|l|m|p|q|d|t|s|?]? ?

Y - (default) Submit the bug report via email.

n - Don't submit the bug report; instead, save it in a temporary file (exits reportbug).

a - Attach a file.

c - Change editor and re-edit.

e - Re-edit the bug report.

i - Include a text file.

l - Pipe the message through the pager.

m - Choose a mailer to edit the report.

p - print message to stdout.

q - Save it in a temporary file and quit.

d - Detach an attachment file.

t - Add tags.

s - Add a X-Debbugs-CC recipient (a CC but after BTS processing).

? - Display this help.

Submit this report on wireshark (e to edit) [Y|n|a|c|e|i|l|m|p|q|d|t|s|?]? Y

Saving a backup of the report at /tmp/reportbug-wireshark-backup-20160328-19073-87oJWJ

Connecting to reportbug.debian.org via SMTP...
```

```
Bug report submitted to: "Debian Bug Tracking System" <submit@bugs.debian.org>

Copies will be sent after processing to:

  buxy@kali.org


If you want to provide additional information, please wait to receive the

bug tracking number via email; you may then send any extra information to

n@bugs.debian.org (e.g. 999999@bugs.debian.org), where n is the bug

number. Normally you will receive an acknowledgement via email including

the bug report number within an hour; if you haven't received a

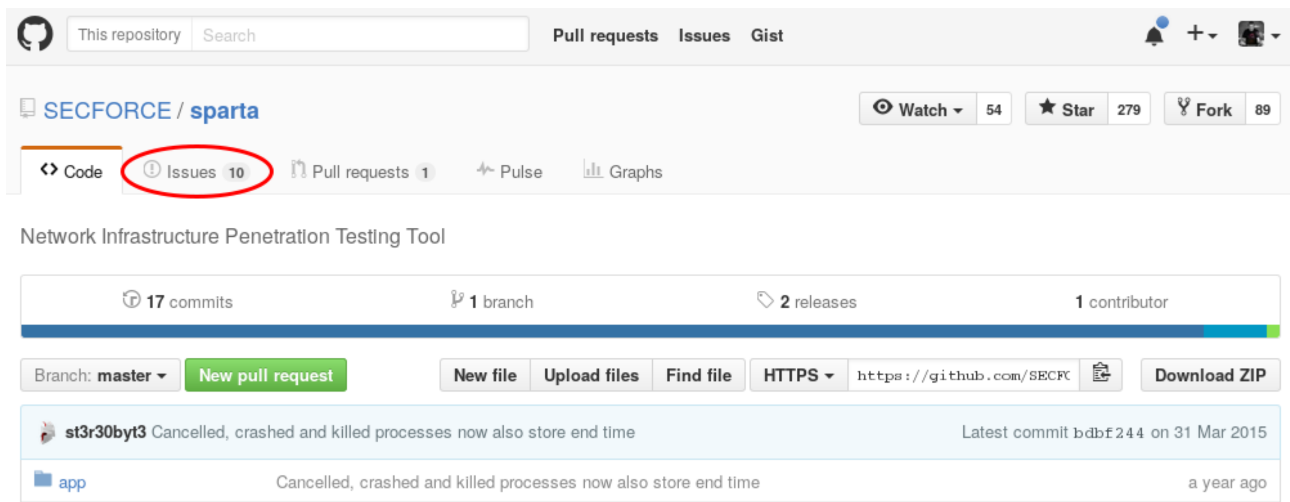
confirmation, then the bug reporting process failed at some point

(reportbug or MTA failure, BTS maintenance, etc.).
```

٦.٣.٣.٣. تقديم تقرير خطأ في مشروع برنامج حر آخر

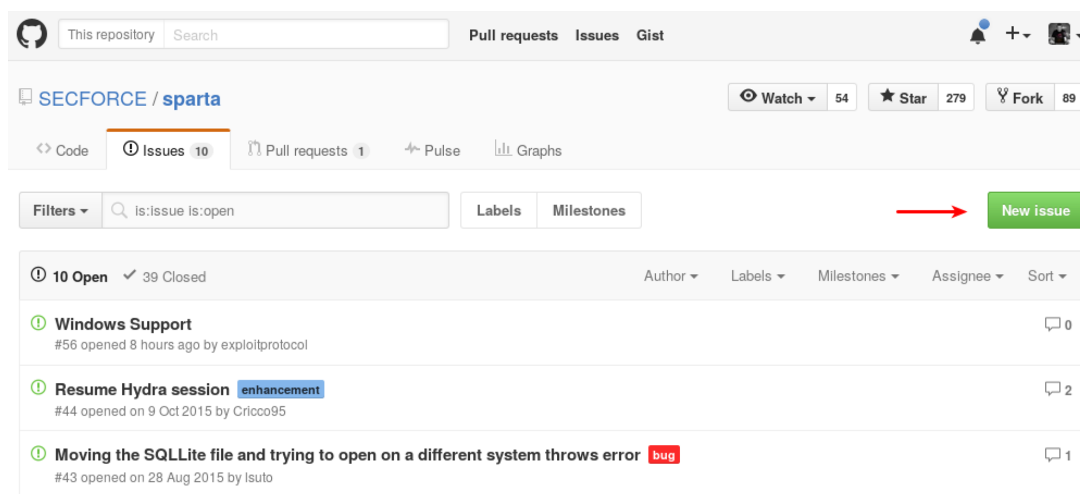
هناك تنوع كبير في مشاريع البرمجيات الحرة، باستخدام سير العمل والأدوات المختلفة. ينطبق هذا التنوع أيضًا على أجهزة تتبع الأخطاء المستخدمة. بينما يتم استضافة العديد من المشاريع على GitHub وتستخدم مشاكل GitHub لتتبع الأخطاء الخاصة بهم، هناك أيضًا العديد من المشاريع الأخرى التي تستضيف برامج التتبع الخاصة بهم، استنادًا إلى Bugzilla و Trac و Redmine و Flyspray وغيرها. معظمها تعتمد على الويب وتتطلب منك تسجيل حساب لإرسال تقرير جديد.

لن نغطي جميع المتعقبات هنا. الأمر متروك لك لمعرفة تفاصيل متتبعات مختلفة لمشاريع برمجيات حرة أخرى، ولكن نظراً لأن GitHub شائع نسبيًا، فسوف نلقي نظرة سريعة عليه هنا. كما هو الحال مع المتعقبات الأخرى، يجب عليك أولاً إنشاء حساب وتسجيل الدخول. بعد ذلك، انقر فوق علامة التبويب المشاكل، كما هو موضح في الشكل ٥.٦، "الصفحة الرئيسية لمشروع GitHub".



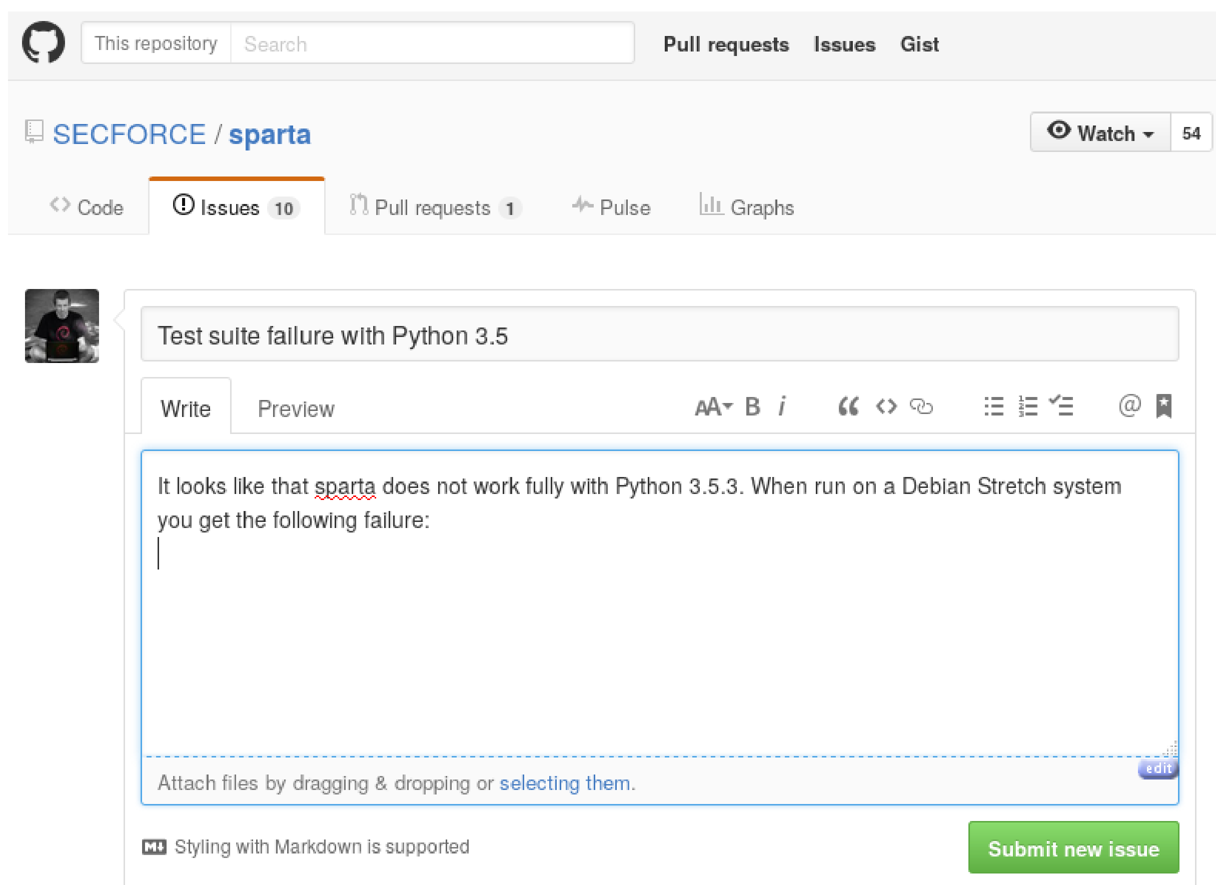
شكل ٥.٦، "الصفحة الرئيسية لمشروع GitHub"

يمكنك بعد ذلك تصفح (والبحث) قائمة المشاكل المفتوحة. بمجرد التأكد من أن الخطأ الخاص بك لم يتم حفظه بعد، يمكنك النقر فوق زر "**New issue**" (الشكل ٦.٦. "صفحة المشاكل الخاصة بمشروع GitHub").



الشكل ٦.٦. صفحة مشكلات مشروع GitHub

أنت الآن في صفحة حيث يجب عليك وصف مشكلتك (الشكل ٧.٦، "نموذج GitHub لتقديم مشكلة جديدة"). على الرغم من عدم وجود قالب مثل النموذج الموجود في reportbug، فإن آلية الإبلاغ عن الأخطاء بسيطة إلى حد ما، مما يسمح لك بإرفاق الملفات وتطبيق التنسيق على النص والمزيد. بالطبع، للحصول على أفضل النتائج، تأكد من اتباع إرشاداتنا لإنشاء تقرير مفصل وموصوف جيدًا.



شكل ٧.٦، "نموذج GitHub لتقديم مشكلة جديدة"

٤.٦ ملخص

ناقشنا في هذا القسم طرقًا مختلفة لمساعدتك في العثور على الوثائق والمعلومات حول البرامج وكيفية العثور على المساعدة بشأن المشكلات التي قد تواجهها. لقد ألقينا نظرة على صفحات **man** و **info** وأوامر **apropos**. ناقشنا أدوات تتبع الأخطاء، وقدمنا بعض النصائح حول كيفية البحث عن تقارير الأخطاء الجيدة وإرسالها، كما قدمنا بعض النصائح لمساعدتك في معرفة من يملك البرنامج أو المشروع المعني.

نصائح تلخيصية:

قبل أن تتمكن من فهم ما يحدث حقًا عند وجود مشكلة، تحتاج إلى معرفة الدور النظري الذي يلعبه كل برنامج مشارك في المشكلة. واحدة من أفضل الطرق للقيام بذلك هي مراجعة وثائق البرنامج.

لعرض صفحة يدوية، ما عليك سوى كتابة **man**، وكتابة اسم الأمر بعد رقم القسم الاختياري.

يعرض الأمر **apropos** قائمة بالصفحات اليدوية التي يذكر ملخصها الكلمات الرئيسية المطلوبة، إلى جانب الملخص المكون من سطر واحد من الصفحة اليدوية.

لقد كتب مشروع GNU أدلة لأغلب برامجه بصيغة المعلومات. هذا هو السبب في أن العديد من الصفحات اليدوية تشير إلى وثائق المعلومات المقابلة.

تحتوي كل حزمة على الوثائق الخاصة بها، وحتى أقل البرامج توثيقًا بشكل عام تحتوي على ملف README يحتوي على بعض المعلومات المهمة. يتم تثبيت هذه الوثائق في المجلد **/usr/share/doc/***package***/**.

في معظم الحالات، قد تعالج الأسئلة الشائعة أو أرشيف القائمة البريدية لموقع الويب الرسمي للبرنامج المشكلات التي واجهتها.

يحتفظ مشروع كالي بمجموعة من الوثائق المفيدة على http://docs.kali.org.

يستخدم مشروع Kali Linux قناة kali-linux#على شبكة Freenode IRC. يمكنك استخدام chat.freenode.net كخادم IRC، على المنفذ 6667 لاتصال مشفر بـ TLS أو المنفذ 6666 لاتصال نص واضح. للانضمام إلى المناقشات حول IRC، يجب عليك استخدام عميل IRC مثل **hexchat** (في الوضع الرسومي) أو **irssi** (في وضع وحدة التحكم). يتوفر أيضًا عميل قائم على الويب على webchat.freenode.net.

توجد منتديات المجتمع الرسمية لمشروع كالي لينكس على forums.kali.org.

إذا كشفت عن خطأ في أحد البرامج، يمكنك البحث في تقارير الأخطاء أو تقديم تقرير خاص بك. تأكد من اتباع الإرشادات التي حددناها للتأكد من أن تقريرك واضح وشامل، ويحسن فرص معالجة المطورين للخطأ في الوقت المناسب.

يجب تقديم بعض تقارير الأخطاء إلى كالي، بينما قد يتم تقديم تقارير أخرى إلى جانب دبيان. أمر مثل `dpkg -s package-name | grep ^Version`: سيكشف عن رقم الإصدار وسيتم وضع علامة عليه باسم "kali" إذا كانت حزمة معدلة من Kali.

عادة ما يكون تحديد مشروع المنبع والعثور على مكان تقديم تقرير الخطأ أمرًا سهلاً. ببساطة تصفح موقع المنبع المشار إليه في حقل Home Page للبيانات الوصفية للتعبئة.

يستخدم Kali أداة تتبع الأخطاء المستندة إلى الويب على https://bugs.kali.org حيث يمكنك استشارة جميع تقارير الأخطاء بشكل مجهول، ولكن إذا كنت ترغب في التعليق أو تقديم تقرير خطأ جديد، فستحتاج إلى تسجيل حساب.

يستخدم دبيان (في الغالب) نظام تتبع الأخطاء المستند إلى البريد الإلكتروني المعروف باسم Debbugs. لفتح تقرير خطأ جديد، يمكنك إرسال بريد إلكتروني (مع بنية خاصة) إلى **Submit@bugs.debian.org** أو يمكنك استخدام الأمر **reportbug**، الذي سيرشدك خلال العملية.

بينما يتم استضافة العديد من المشاريع على GitHub وتستخدم GitHub Issues لتتبع الأخطاء، هناك أيضًا العديد من المشاريع الأخرى التي تستضيف برامج التتبع الخاصة بهم. قد تضطر إلى البحث في أساسيات أجهزة تتبع الأخطاء التابعة لجهات خارجية إذا كنت تريد النشر عليها.

الآن بعد أن حصلت على الأدوات الأساسية للتنقل في Linux، وتثبيت Kali وتكوينه، واستكشاف أخطاء النظام وإصلاحها والحصول على المساعدة، حان الوقت للنظر في قفل Kali حتى تتمكن من حماية التثبيت بالإضافة إلى بيانات العميل.

التمرين الأول – للفصل السادس – موارد كالي

١. تريد معرفة ما إذا كان إصدار xyz$ الإصدار الأخير من **nmap** في كالي. ما هو أسرع مورد كالي للتحقق من ذلك؟
٢. ما هما المصدران الأساسيان التفاعليان لدعم مجتمع كالي؟
٣. كيف تبحث في الصفحات اليدوية عن نص معينة؟

الإجابة:

١. لماذا، بالطبع، سيكون ذلك pkg.kali.org. على سبيل المثال، http://pkg.kali.org/nmap.
٢. قناة Kali-Linux IRC# على Freenode ومنتديات Kali.
٣. استخدم الأمر **apropos**.

اختبار الشهادة للفصل السادس

أي أمر سيحدد ما إذا تم تعديل **nmap** بواسطة Kali؟

- **dpkg -l | grep nmap**
- **dpkg -s nmap | grep ^Version**
- **dpkg-query -l | grep nmap**
- جميع ما سبق
- جميع الإجابات خاطئة

ما هو الأمر المستخدم للإبلاغ عن خطأ لمطوري ديبان؟

kalibug

bugreport

reportbug

irssi

أي من هذه الإجراءات يمكن استخدامها لإرسال خطأ لمطوري ديبان؟

- Use the official Debian bug tracker at https://bugs.debian.org
- Send an email (with a special syntax) to submit@bugs.debian.org
- Use the kalidebug tool directly from Kali Linux and mark the issue as an upstream Debian issue.
- أرسل الخلل إلى متتبع أخطاء Kali الرسمي على https://bugs.kali.org وضع علامة على مشكلة تصحيح دیبیان.

الإجابة:

1

- كل ما سبق

2

- **`reportbug`**

3

- Use the official Debian bug tracker at https://bugs.debian.org
- Send an email (with a special syntax) to submit@bugs.debian.org
- Submit the bug to the official Kali bug tracker at https://bugs.kali.org and mark the issue for an upstream Debian patch.

---((الفصل السابع))---

٧. تأمين ومراقبة KALI

عندما تبدأ في استخدام Kali Linux للعمل الذي يزداد حساسية وخصوصية، ستحتاج على الأرجح إلى أخذ أمان التثبيت بجدية أكبر. في هذا الفصل، سنناقش أولاً السياسات الأمنية، مع تسليط الضوء على النقاط المختلفة التي يجب مراعاتها عند تحديد مثل هذه السياسة، وتحديد بعض التهديدات لنظامك ولك بصفتك محترف أمان. سنناقش أيضًا الإجراءات الأمنية لأنظمة الحاسوب المحمول وأجهزة الحاسوب المكتبية ونركز على الجدران النارية وتصفية الحزم. أخيرًا، سنناقش أدوات واستراتيجيات المراقبة ونوضح لك أفضل طريقة لتطبيقها لاكتشاف التهديدات المحتملة لنظامك.

١.٧. تحديد سياسة الأمن

من غير العملي مناقشة الأمن بنقاط ثابتة لأن الفكرة تمثل مجموعة واسعة من المفاهيم والأدوات والإجراءات، والتي لا ينطبق أي منها عالميًا. يتطلب الاختيار من بينها فكرة دقيقة عن أهدافك. يبدأ تأمين النظام بالإجابة على بعض الأسئلة. الاندفاع بتهور نحو تنفيذ مجموعة من الأدوات التعسفية إلى خطر التركيز على الجوانب الخاطئة للأمن.

عادة ما يكون من الأفضل تحديد هدف معين. يبدأ النهج الجيد للمساعدة في هذا التصميم بالأسئلة التالية:

ما الذي تحاول حمايته؟ ستختلف سياسة الأمان اعتمادًا على ما إذا كنت ترغب في حماية أجهزة الحاسوب أو البيانات. في حالة البيانات، تحتاج أيضًا إلى معرفة البيانات.

ما الذي تحاول حمايته؟ هل هو تسرب البيانات السرية؟ فقدان البيانات العرضية؟ خسارة الإيرادات بسبب انقطاع الخدمة؟

أيضا، من الذي تحاول الحماية منه؟ ستكون الإجراءات الأمنية مختلفة تمامًا للحماية من خطأ مطبعي من قبل مستخدم عادي للنظام مقابل الحماية ضد مجموعة مهاجمين من الخارج.

يُستخدم مصطلح "الخطر "risk"" عادة للإشارة بشكل عام لهذه العوامل الثلاثة:

ما الذي يجب حمايته، وما الذي يجب منعه، ومن الذي قد يحدث ذلك.

تتطلب نمذجة المخاطر إجابات على هذه الأسئلة الثلاثة. من نموذج المخاطر هذا، يمكن بناء سياسة أمنية وتنفيذ السياسة بإجراءات ملموسة.

تحقق دائما

يحاول بروس شناير، الخبير العالمي في شؤون الأمن (ليس فقط أمن الحاسوب)، مواجهة واحدة من أهم خرافات الأمن بشعار: "الأمن عملية وليس منتجًا". تتغير الموارد المطلوب حمايتها بمرور الوقت وكذلك تتغير التهديدات والوسائل المتاحة للمهاجمين. حتى لو تم تصميم وتنفيذ سياسة أمنية بشكل مثالي في البداية، يجب ألا ترتاح أبداً. تتطور مكونات الخطر ويجب أن تتطور الاستجابة لذلك الخطر وفقًا لذلك.

تستحق القيود الإضافية أيضًا أن تؤخذ في الاعتبار، لأنها يمكن أن تحد من نطاق السياسات المتاحة. إلى أي مدى أنت على استعداد لتأمين النظام؟ هذا السؤال له تأثير كبير على السياسة التي يتعين تنفيذها. في كثير من الأحيان، يتم تحديد الإجابة فقط من حيث التكاليف النقدية، ولكن يجب أيضًا مراعاة عناصر أخرى، مثل مقدار الإزعاج المفروض على مستخدمي النظام أو تدهور الأداء.

بمجرد نمذجة الخطر، يمكنك البدء في التفكير في تصميم سياسة أمنية حقيقية.

هناك حالات شاذة يمكن أن تلعب دورها عند تحديد مستوى الحماية الأمنية التي يجب اعتمادها. من ناحية، يمكن أن يكون من السهل للغاية توفير أمان النظام الأساسي.

على سبيل المثال، إذا كان النظام المراد حمايته يتألف فقط من حاسوب مستعمل، يكون استخدامه الوحيد هو إضافة عدد قليل من الأرقام في نهاية اليوم، فإن اتخاذ قرار بعدم القيام بأي شيء خاص لحمايته سيكون أمرًا معقولًا تمامًا. القيمة الجوهرية للنظام منخفضة وقيمة البيانات صفر حيث لا يتم تخزينها على الحاسوب. المهاجم المحتمل التسلل إلى هذا النظام سيحصل على آلة حاسبة فقط. من المحتمل أن تكون تكلفة تأمين مثل هذا النظام أكبر من تكلفة الخرق.

في الطرف الآخر من النطاق، قد ترغب في حماية سرية البيانات السرية بأكثر طريقة شاملة ممكنة، متفوقة على أي اعتبار آخر. في هذه الحالة، سيكون الرد المناسب هو التدمير الكامل للبيانات (محو الملفات بشكل آمن، وتمزيق الأقراص الصلبة إلى أجزاء، ثم إذابة هذه الأجزاء في الحمض، وما إلى ذلك). إذا كان هناك مطلب إضافي بوجوب حفظ البيانات في المخزن للاستخدام المستقبلي (على الرغم من عدم توفرها بسهولة بالضرورة)، وإذا لم تكن التكلفة عاملاً، فستكون نقطة البداية هي تخزين البيانات على لوحات سبائك إيريديوم - بلاتينيوم المخزنة في مخابئ واقية من القنابل تحت جبال مختلفة في العالم، كل منها (بالطبع) سرية تمامًا وتحرسها جيوش بأكملها.

على الرغم من أن هذه الأمثلة قد تبدو شاذة، إلا أنها قد تكون استجابة كافية لبعض المخاطر المحددة، بقدر ما هي نتيجة عملية فكرية تأخذ في الاعتبار الأهداف التي يجب الوصول إليها والقيود التي يجب تحقيقها. عند اتخاذ قرار منطقي، لا توجد سياسة أمنية محترمة أكثر أو أقل من أي سياسة أخرى.

بالعودة إلى حالة أكثر نموذجية، يمكن تقسيم نظام المعلومات إلى أنظمة فرعية متسقة ومعظمها مستقلة. سيكون لكل نظام فرعي متطلباته وقيوده الخاصة، وبالتالي يجب إجراء تقييم المخاطر وتصميم السياسة الأمنية بشكل منفصل لكل منهما. من المبادئ الجيدة التي يجب وضعها في الاعتبار أن سطح الهجوم الصغير أسهل في الدفاع عنه من السطح الكبير. يجب أيضًا أن يتم تصميم تنظيم الشبكة وفقًا لذلك: يجب أن تركز الخدمات الحساسة على عدد صغير من الأجهزة، ويجب ألا يمكن الوصول إلى هذه الأجهزة إلا من خلال الحد الأدنى من المسارات أو نقاط التفتيش. المنطق واضح: من الأسهل تأمين نقاط التفتيش هذه من تأمين جميع الآلات الحساسة ضد العالم الخارجي بأكمله. عند هذه النقطة تظهر فائدة تصفية الشبكة (بما في ذلك جدران الحماية). يمكن تنفيذ هذا التصفية باستخدام أجهزة مخصصة ولكن الحل الأبسط والأكثر مرونة هو استخدام برنامج جدار حماية مثل ذلك الذي تم دمجه في نواة Linux.

٢.٧. التدابير الأمنية الممكنة

كما أوضح الباب السابق، لا يوجد رد واحد على السؤال حول كيفية تأمين Kali Linux. كل هذا يتوقف على كيفية استخدامه وما تحاول حمايته.

١.٢.٧. على الخادم

إذا قمت بتشغيل Kali Linux على خادم يمكن الوصول إليه بشكل عام، فأنت على الأرجح ترغب في تأمين خدمات الشبكة عن طريق تغيير أي كلمات مرور افتراضية يمكن تكوينها (انظر القسم ٣.٧، "تأمين خدمات الشبكة") وربما أيضًا عن طريق تقييد وصولهم بجدار حماية (راجع القسم ٤.٧، "جدار الحماية أو تصفية الحزم").

إذا قمت بتوزيع حسابات المستخدمين إما مباشرة على الخادم أو على إحدى الخدمات، فأنت تريد التأكد من تعيين كلمات مرور قوية (يجب أن تقاوم هجمات القوة الغاشمة). في الوقت نفسه، قد ترغب في إعداد *fail2ban*، الذي سيجعل الأمر أكثر صعوبة هجمات القوة الغاشمة عبر الشبكة (من خلال تصفية عناوين IP التي تتجاوز حد محاولات تسجيل الدخول الفاشلة). قم بتثبيت *fail2ban* بـ **apt update** يليه **apt install fail2ban**.

إذا قمت بتشغيل خدمات الويب، فربما تريد استضافتها عبر HTTPS لمنع وسطاء الشبكة من استنشاق حركة المرور الخاصة بك (والتي قد تتضمن ملفات تعريف ارتباط المصادقة).

٢.٢.٧. على جهاز حاسوب محمول

لا يخضع الحاسوب المحمول الخاص بأداة اختبار الاختراق لنفس المخاطر التي يتعرض لها الخادم العام: على سبيل المثال، يقل احتمال تعرضك لعمليات مسح عشوائية من أطفال البرامج النصية وحتى عندما تكون كذلك، فربما لن يكون لديك أي خدمات شبكة ممكّنة.

غالبًا ما تنشأ المخاطر الحقيقية عند السفر من عميل إلى آخر. على سبيل المثال، يمكن سرقة الحاسوب المحمول أثناء السفر أو الاستيلاء عليه من قبل الجمارك. هذا هو السبب في أنك على الأرجح ترغب في استخدام تشفير كامل للقرص (انظر القسم ٢.٢.٤، "التثبيت على نظام ملفات مشفر بالكامل") وربما أيضًا إعداد ميزة "nuke": البيانات التي جمعتها أثناء ارتباطاتك سرية وتتطلب أقصى درجات الحماية.

قد تحتاج أيضًا إلى قواعد جدار الحماية (انظر القسم ٤.٧، "جدار الحماية أو تصفية الحزم") ولكن ليس للغرض نفسه كما في الخادم. قد ترغب في منع كل حركة المرور الصادرة باستثناء حركة المرور الناتجة عن وصول VPN الخاص بك. يُقصد بهذا كشبكة أمان، بحيث عندما تعطل الشبكة الافتراضية الخاصة، تلاحظها على الفور (بدلاً من العودة إلى الوصول إلى الشبكة المحلية). وبهذه الطريقة، لا تفشي عناوين IP الخاصة بعملائك عند تصفح الويب أو القيام بأنشطة أخرى عبر الإنترنت. بالإضافة إلى ذلك، إذا كنت تؤدي مشاركة داخلية محلية، فمن الأفضل أن تظل متحكمًا في جميع أنشطتك لتقليل الضوضاء التي تحدثها على الشبكة، والتي يمكن أن تنبه العميل وأنظمة الدفاع الخاصة به.

٣.٧. تأمين خدمات الشبكة

بشكل عام، يعد تعطيل الخدمات التي لا تستخدمها فكرة جيدة. يسهّل Kali القيام بذلك نظراً لأن معظم خدمات الشبكة معطلة افتراضياً.

طالما أن الخدمات لا تزال معطلة، فإنها لا تشكل أي تهديد أمني. ومع ذلك، يجب أن تكون حذرًا عند تمكينها للأسباب التالية:

١. لا يوجد جدار حماية افتراضياً، لذلك إذا استمعوا إلى جميع واجهات الشبكة، فستكون متاحة للجمهور بشكل نشط.
٢. لا تحتوي بعض الخدمات على بيانات اعتماد المصادقة وتتيح لك تعيينها عند الاستخدام الأول؛ الآخرون لديهم بيانات اعتماد افتراضية (وبالتالي معروفة على نطاق واسع). تأكد من (إعادة) تعيين أي كلمة مرور لشيء تعرفه أنت فقط.
٣. تعمل العديد من الخدمات كجذر مع امتيازات المسؤول الكاملة، وبالتالي فإن عواقب الوصول غير المصرح به أو خرق الأمان عادة ما تكون شديدة.

الشهادات الإفتراضية

لن نذكر هنا جميع الأدوات التي تأتي مع الشهادات الافتراضية، بدلاً من ذلك يجب عليك التحقق من ملف README.Debian للحزم المعنية، وكذلك docs.kali.org و tools.kali.org لمعرفة ما إذا كانت الخدمة تحتاج إلى بعض الميزات الخاصة الحرص على تأمينها.

إذا كنت تعمل في الوضع المباشر، فإن كلمة مرور الحساب الجذر هي "toor". وبالتالي، يجب ألا تقوم بتمكين SSH قبل تغيير كلمة المرور للحساب الجذر، أو قبل أن تعدل تكوينها لعدم السماح بتسجيلات الدخول المستندة إلى كلمة المرور.

لاحظ أيضًا أن مشروع BeEF (من الحزمة المثبتة بالفعل beef-xss) معروف أيضا بامتلاكه لبيانات الاعتماد الافتراضية "beef" ، كلمة المرور "beef") في ملف التكوين الافتراضي الخاص به.

4.7. جدار الحماية أو تصفية الحزم

جدار الحماية هو قطعة من أجهزة الحاسوب التي تحتوي على أجهزة أو برامج أو كليهما يوزع حزم الشبكة الواردة أو الصادرة (القادمة من شبكة محلية أو المغادرة منها) ويسمح فقط من خلال تلك المطابقة لشروط معينة محددة مسبقًا.

بوابة شبكة التصفية هي نوع من جدار الحماية الذي يحمي شبكة كاملة. عادة ما يتم تثبيته على جهاز مخصص تم تكوينه كبوابة للشبكة بحيث يمكنه تحليل جميع الحزم التي تمر من وإلى الشبكة. بدلاً من ذلك، يعد جدار الحماية المحلي خدمة برمجية يتم تشغيلها على جهاز معين من أجل تصفية أو تقييد الوصول إلى بعض الخدمات على هذا الجهاز، أو ربما لمنع الاتصالات الصادرة عن طريق برنامج خبيث يمكن للمستخدم تثبيته، سواء عن قصد أو بدونه.

تشتمل نواة Linux على جدار الحماية *netfilter*. لا يوجد حل جاهز لتكوين أي جدار حماية نظراً لاختلاف متطلبات الشبكة والمستخدم. ومع ذلك، يمكنك التحكم في netfilter من مساحة المستخدم باستخدام أوامر **iptables** و **ip6tables**. الفرق بين هذين الأمرين هو أن الأول يعمل لشبكات IPv4، بينما يعمل الأخير على IPv6؛ نظراً لأن مكدسي بروتوكولات الشبكة قد يكونان متاحين لسنوات عديدة، فستحتاج كلتا الأداتين إلى الاستخدام بالتوازي. يمكنك أيضًا استخدام أداة **fwbuilder** الممتازة المستندة إلى واجهة المستخدم الرسومية، والتي توفر تمثيلًا رسومياً لقواعد التصفية.

ومع ذلك، قررت تكوينه، netfilter هو تطبيق جدار حماية Linux، لذلك دعونا نلقي نظرة فاحصة على كيفية عمله.

١.٤.٧. سلوك Netfilter

تستخدم Netfilter أربعة جداول مميزة، تخزن القواعد التي تنظم ثلاثة أنواع من العمليات على الحزم:

filter: يتعلق بقواعد التصفية (قبول الحزمة أو رفضها أو تجاهلها).

nat: (ترجمة عنوان الشبكة "Network Address Translation") تتعلق بترجمة عناوين المصدر أو الوجهة ومنافذ الحزم.

mangle: يتعلق بتغييرات أخرى لحزم IP (بما في ذلك ToS - نوع الخدمة - الحقل والخيارات).

raw: يسمح بتعديلات يدوية أخرى على الحزم قبل وصولها إلى نظام تتبع الاتصال.

يحتوي كل جدول على قوائم قواعد تسمى *السلاسل "chains"*. يستخدم جدار الحماية سلاسل قياسية للتعامل مع الحزم بناءً على ظروف محددة مسبقًا. يمكن للمسؤول إنشاء سلاسل أخرى، والتي سيتم استخدامها فقط عند الإشارة إليها بواسطة إحدى السلاسل القياسية (سواء بشكل مباشر أو غير مباشر).

يحتوي جدول filter على ثلاث سلاسل قياسية:

INPUT: يتعلق بالحزم التي يكون وجهتها الجدار الناري نفسه.

OUTPUT: يتعلق بالحزم المنبعثة من جدار الحماية.

FORWARD: تتعلق الحزم التي تمر عبر جدار الحماية (وهو ليس مصدرها ولا وجهتها).

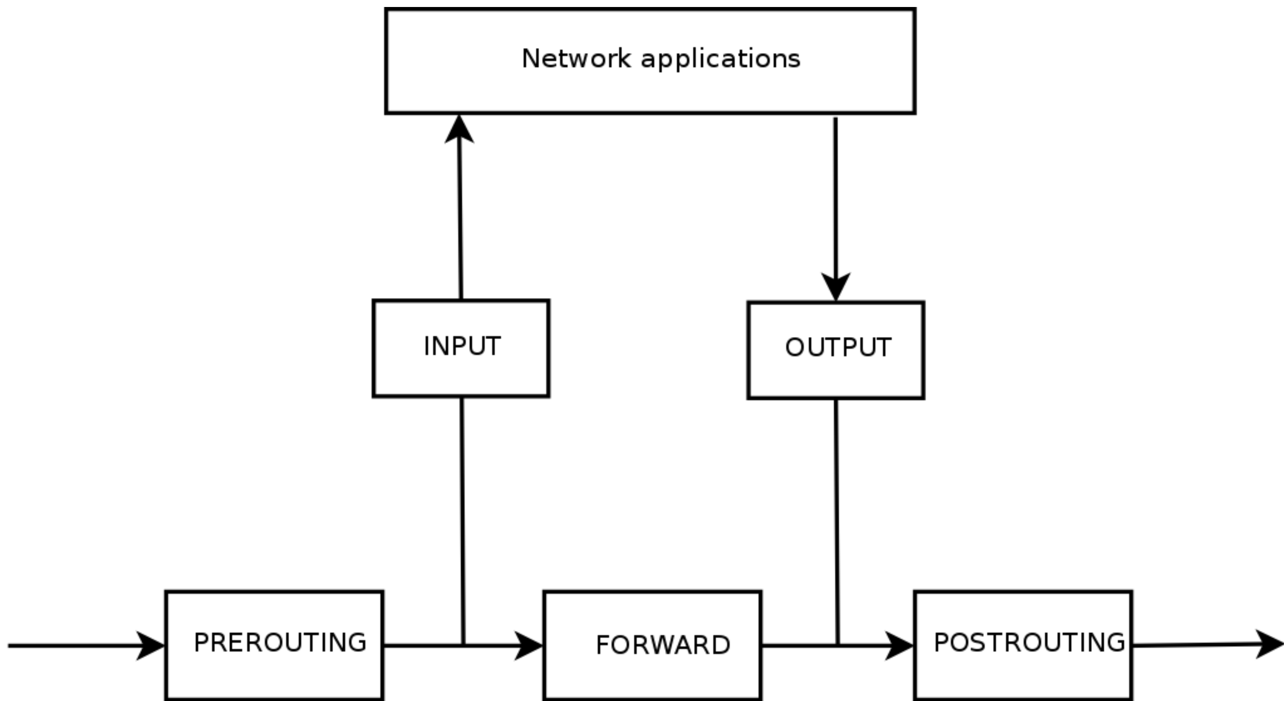
يحتوي جدول nat أيضًا على ثلاث سلاسل قياسية:

PREROUTING: تعديل الحزم بمجرد وصولها.

POSTROUTING: تعديل الحزم عندما تكون جاهزة للذهاب في طريقها.

OUTPUT (الإخراج): لتعديل الحزم التي تم إنشاؤها بواسطة جدار الحماية نفسه.

يتم توضيح هذه السلاسل في الشكل ١.٧، "كيف يتم استدعاء سلاسل Netfilter".



الشكل ١.٧. كيف يتم استدعاء سلاسل Netfilter

كل سلسلة قائمة بالقواعد. كل قاعدة هي مجموعة من الشروط وإجراء للقيام به عند استيفاء الشروط. عند معالجة حزمة، يقوم جدار الحماية بمسح السلسلة المناسبة، وقاعدة تلو الأخرى، وعندما يتم استيفاء الشروط لقاعدة واحدة، فإنه يقفز (ومن ثم يكون الخيار j- في الأوامر) إلى

الإجراء المحدد لمتابعة المعالجة. السلوكيات الأكثر شيوعًا هي إجراءات موحدة ومخصصة لهم. يؤدي اتخاذ أحد هذه الإجراءات القياسية إلى مقاطعة معالجة السلسلة، لأن مصير الحزم مختوم بالفعل (باستثناء الاستثناء المذكور أدناه). فيما يلي إجراءات Netfilter.

ACCEPT: السماح للحزمة في طريقها.

REJECT: رفض الحزمة باستخدام حزمة خطأ بروتوكول رسائل التحكم في الإنترنت (ICMP) (يحدد خيار reject-with type-- من iptables نوع الخطأ الذي سيتم إرساله).

DROP: حذف (تجاهل) الحزمة.

LOG: تسجيل (عبر syslogd) رسالة مع وصف الحزمة. لاحظ أن هذا الإجراء لا يقاطع العملية، ويستمر تنفيذ السلسلة في القاعدة التالية، وهذا هو السبب في أن تسجيل الحزم المرفوضة يتطلب كلاً من LOG وقاعدة REJECT / DROP. تشمل المعلمات الشائعة المرتبطة بالتسجيل ما يلي:

log-level--، مع القيمة الافتراضية تحذير "warning"، يشير إلى مستوى خطورة سجل النظام.

يسمح **log-prefix**-- بتحديد بادئة نصية للتمييز بين الرسائل المسجلة.

يشير كل من **log-tcp-sequence**-- و **log-tcp-options**-- و **log-ip-options**-- إلى بيانات إضافية يتم دمجها في الرسالة: على التوالي رقم تسلسل TCP وخيارات TCP وخيارات IP.

ULOG: تسجيل رسالة عبر ulogd، والتي يمكن تكييفها بشكل أفضل وأكثر كفاءة من syslogd للتعامل مع أعداد كبيرة من الرسائل؛ لاحظ أن هذا الإجراء، مثل LOG، يعيد أيضًا المعالجة إلى القاعدة التالية في سلسلة الاستدعاء.

chain_name: القفز إلى السلسلة المعينة وتقييم قواعدها.

RETURN: مقاطعة عملية السلسلة الحالية والعودة إلى سلسلة الاستدعاء؛ في حالة أن السلسلة الحالية هي سلسلة قياسية، لا توجد سلسلة اتصال، لذلك يتم تنفيذ الإجراء الافتراضي (المحدد بخيار P- إلى iptables) بدلاً من ذلك.

SNAT (فقط في جدول **nat**): تطبيق ترجمة عنوان شبكة المصدر (SNAT). تصف الخيارات الإضافية التغييرات الدقيقة لتطبيقها، بما في ذلك خيار to-source address: port--، الذي يحدد عنوان IP المصدر الجديد و / أو المنفذ.

DNAT (فقط في جدول **nat**): تطبيق ترجمة عنوان شبكة الوجهة (DNAT). تصف الخيارات الإضافية التغييرات الدقيقة لتطبيقها، بما في ذلك خيار to-destination *address:port*--، الذي يحدد عنوان IP الجديد للوجهة و / أو المنفذ.

MASQUERADE (فقط في جدول **nat**): تطبيق التنكر "masquerading " (حالة خاصة من Source NAT).

REDIRECT (فقط في جدول **nat**): إعادة توجيه حزمة بشفافية إلى منفذ معين من جدار الحماية نفسه؛ يمكن استخدام هذا لإعداد وكيل ويب شفاف يعمل بدون تكوين على جانب العميل، حيث يعتقد العميل أنه يتصل بالمستلم بينما تمر الاتصالات فعلياً عبر الوكيل. يشير خيار **to-ports** *port(s)*--إلى المنفذ، أو نطاق المنفذ، حيث يجب إعادة توجيه الحزم.

الإجراءات الأخرى، وخاصة تلك المتعلقة بالجدول **mangle**، تقع خارج نطاق هذا النص. تحتوي صفحات iptables(8) و (8) ip6tables على قائمة شاملة.

ما هو ICMP؟

بروتوكول رسائل التحكم في الإنترنت (ICMP) هو البروتوكول المستخدم لإرسال المعلومات الإضافية عن الاتصالات. يختبر اتصال الشبكة باستخدام الأمر **ping**، الذي يرسل رسالة طلب صدى "ICMP "echo request، والتي من المفترض أن يجيب عليها المستلم برسالة رد صدى "ICMP "echo reply. يشير إلى جدار حماية يرفض حزمة، ويشير إلى تجاوز سعة في المخزن المؤقت للاستلام، ويقترح مسارًا أفضل للحزم التالية في الاتصال، وما إلى ذلك. يتم تعريف هذا البروتوكول من خلال العديد من وثائق RFC. كان RFC777 و RFC792 الأول، ولكن العديد من الآخرين وسعوا و/أو راجعوا البروتوكول.

http://www.faqs.org/rfcs/rfc777.html

http://www.faqs.org/rfcs/rfc792.html

كمرجع، يعد المخزن المؤقت للاستلام منطقة ذاكرة صغيرة تخزن البيانات بين الوقت الذي تصل فيه من الشبكة والوقت الذي تعالجه فيه النواة. إذا كانت هذه المنطقة ممتلئة، فلا يمكن تلقي بيانات جديدة وتشير ICMP إلى المشكلة بحيث يمكن للمرسل إبطاء معدل النقل (الذي يجب أن يصل إلى التوازن بشكل مثالي بعد مرور بعض الوقت).

لاحظ أنه على الرغم من أن شبكة IPv4 يمكن أن تعمل بدون ICMP، إلا أن ICMPv6 مطلوب بشدة لشبكة IPv6، نظرًا لأنه يجمع بين العديد من الوظائف التي انتشرت في عالم IPv4 عبر ICMPv4 وبروتوكول عضوية مجموعة الإنترنت " Internet Group Membership Protocol" (IGMP) وبروتوكول تحليل العنوان (ARP).

تم تعريف ICMPv6 في RFC4443.

http://www.faqs.org/rfcs/rfc4443.html

٧.٤.٢. بناء الجملة من iptables و ip6tables

يتم استخدام أوامر **iptables** و **ip6tables** لمعالجة الجداول والسلاسل والقواعد. يشير خيار **t table-** الخاص بهم إلى الجدول الذي سيعمل عليه (بشكل افتراضي، **filter**).

٧.٤.٢.١. أوامر

الخيارات الرئيسية للتفاعل مع السلاسل:

chain **L-** : يسرد القواعد في السلسلة. يُستخدم هذا عادةً مع الخيار **n-** لتعطيل تحليل الاسم (على سبيل المثال، **iptables -n -L INPUT** سيعرض القواعد المتعلقة بالحزم الواردة).

chain **N-** : ينشئ سلسلة جديدة. يمكنك إنشاء سلاسل جديدة لعدد من الأغراض، بما في ذلك اختبار خدمة شبكة جديدة أو صد هجوم على الشبكة.

chain **X-** : تحذف سلسلة فارغة وغير مستخدمة (على سبيل المثال، iptables -X ddos-attack).

chain rule **A-** : يضيف قاعدة في نهاية السلسلة المعطاة. تذكر أن القواعد تتم معالجتها من الأعلى إلى الأسفل، لذا تأكد من مراعاة ذلك عند إضافة القواعد.

chain rule_num rule **I-** : يدرج قاعدة قبل القاعدة رقم Rule_num. كما هو الحال مع الخيار **A-** ، ضع أمر المعالجة في الاعتبار عند إدراج قواعد جديدة في سلسلة.

`-D chain rule_num (or -D chain rule)`: تحذف قاعدة في سلسلة؛ تحدد الصيغة الأولى القاعدة التي سيتم حذفها من خلال رقمها (**iptables -L --line-numbers** ستعرض أرقام الأسطر)، بينما يحددها الأخير من خلال محتوياته.

-F *chain* : مسح سلسلة (حذف كافة قواعدها). على سبيل المثال، لحذف جميع القواعد المتعلقة بالحزم الصادرة، يمكنك تشغيل `iptables -F OUTPUT`. إذا لم يتم ذكر سلسلة، يتم حذف جميع القواعد في الجدول.

-P *chain action* يحدد الإجراء الافتراضي، أو "السياسة" لسلسلة معينة؛ لاحظ أن السلاسل القياسية فقط يمكن أن يكون لها مثل هذه السياسة. لإسقاط كل حركة المرور الواردة بشكل افتراضي، ستقوم بتشغيل `iptables -P INPUT DROP`.

٢.٢.٤.٧. قواعد

يتم التعبير عن كل قاعدة كـ *conditions* **-j** *action action_options*. إذا تم وصف العديد من الشروط في نفس القاعدة، فإن المعيار هو اقتران (logical *AND*) الشروط، والتي تكون على الأقل مقيدة مثل كل حالة على حدة.

يطابق شرط **-p** *protocol* مجال بروتوكول حزمة IP. القيم الأكثر شيوعًا هي tcp و udp و icmp و icmpv6. يمكن استكمال هذا الشرط بشروط على منافذ TCP، مع عبارات مثل: **--source-port** *port* و **--destination-port** *port*.

شروط سلبية

يؤدي إجراء شرط مسبق بعلامة تعجب إلى إبطال الشرط. على سبيل المثال: يتعارض رفض شرط في الخيار p- مع "أي حزمة ببروتوكول مختلف عن البروتوكول المحدد". يمكن تطبيق آلية النفي هذه على جميع الشروط الأخرى أيضًا.

يتطابق شرط **s** *address*- أو **s** *network/mask*- مع عنوان مصدر الحزمة. بالمقابل، فإن **d** *address* - أو **d** *network/mask*- يطابق عنوان الوجهة.

يختار شرط **i** *interface*- الحزم القادمة من واجهة الشبكة المحددة. **o** *interface*- تختار الحزم التي تخرج على واجهة معينة.

يطابق شرط **state** *state*-- حالة الحزمة في اتصال (وهذا يتطلب وحدة **ipt_conntrack** النواة لتتبع الاتصال). تصف الحالة **NEW** حزمة تبدأ اتصالًا جديدًا، وتتطابق **ESTABLISHED** مع الحزم التي تنتمي إلى اتصال موجود بالفعل، وتتطابق **RELATED** مع الحزم التي تبدأ اتصالًا جديدًا متعلقًا باتصال موجود (وهو أمر مفيد لاتصالات **ftp-data** في الوضع "النشط") بروتوكول FTP).

هناك العديد من الخيارات المتاحة ل **iptables** و **ip6tables** وإتقانها كلها تتطلب قدرا كبيرا من الدراسة والخبرة. ومع ذلك، فإن أحد الخيارات التي ستستخدمها في الغالب هو

حظر حركة مرور الشبكة الضارة من مضيف أو مجموعة من المضيفين. على سبيل المثال، لحظر حركة المرور الواردة بصمت من عنوان ip 10.0.1.5 والشبكة الفرعية من الفئة C :31.13.74.0/24

```
# iptables -A INPUT -s 10.0.1.5 -j DROP
# iptables -A INPUT -s 31.13.74.0/24 -j DROP
# iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.1.5             0.0.0.0/0
DROP       all  --  31.13.74.0/24        0.0.0.0/0
```

أمر **iptables** آخر شائع الاستخدام هو السماح بحركة مرور الشبكة لخدمة أو منفذ معين. للسماح للمستخدمين بالاتصال بـ SSH و HTTP و IMAP، يمكنك تشغيل الأوامر التالية:

```
# iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
# iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
# iptables -A INPUT -m state --state NEW -p tcp --dport 143 -j ACCEPT
# iptables -n -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.1.5             0.0.0.0/0
DROP       all  --  31.13.74.0/24        0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:143
```

تعتبر النظافة الجيدة للحاسوب لتنظيف القواعد القديمة وغير الضرورية. أسهل طريقة لحذف قواعد **iptables** هي الرجوع إلى القواعد حسب رقم السطر، والتي يمكنك استرجاعها باستخدام خيار **line-numbers--**. كن حذرًا على الرغم من ذلك: سيؤدي إسقاط قاعدة إلى إعادة ترقيم جميع القواعد التي تظهر بشكل أكبر في السلسلة.

```
# iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  10.0.1.5             0.0.0.0/0
2    DROP       all  --  31.13.74.0/24        0.0.0.0/0
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:143
# iptables -D INPUT 2
# iptables -D INPUT 1
# iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
2    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:80
3    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:143
```

هناك شروط أكثر تحديدًا، اعتمادًا على الشروط العامة الموضحة أعلاه. لمزيد من المعلومات، راجع (8) iptables و (8) ip6tables.

٣.٤.٧. إنشاء قواعد

تتطلب كل عملية إنشاء قاعدة استدعاء **iptables** أو **ip6tables**. قد تكون كتابة هذه الأوامر يدويًا مملة، لذلك يتم تخزين المكالمات عادة في برنامج نصي بحيث يتم تكوين النظام تلقائيًا بنفس الطريقة في كل مرة يتم فيها تشغيل الجهاز. يمكن كتابة هذا البرنامج النصي يدويًا ولكن قد يكون من المفيد أيضًا إعداده باستخدام أداة عالية المستوى مثل **fwbuilder**.

```
# apt install fwbuilder
```

المبدأ بسيط. في الخطوة الأولى، صف جميع العناصر التي ستشارك في القواعد الفعلية:

جدار الحماية نفسه، مع واجهات شبكته

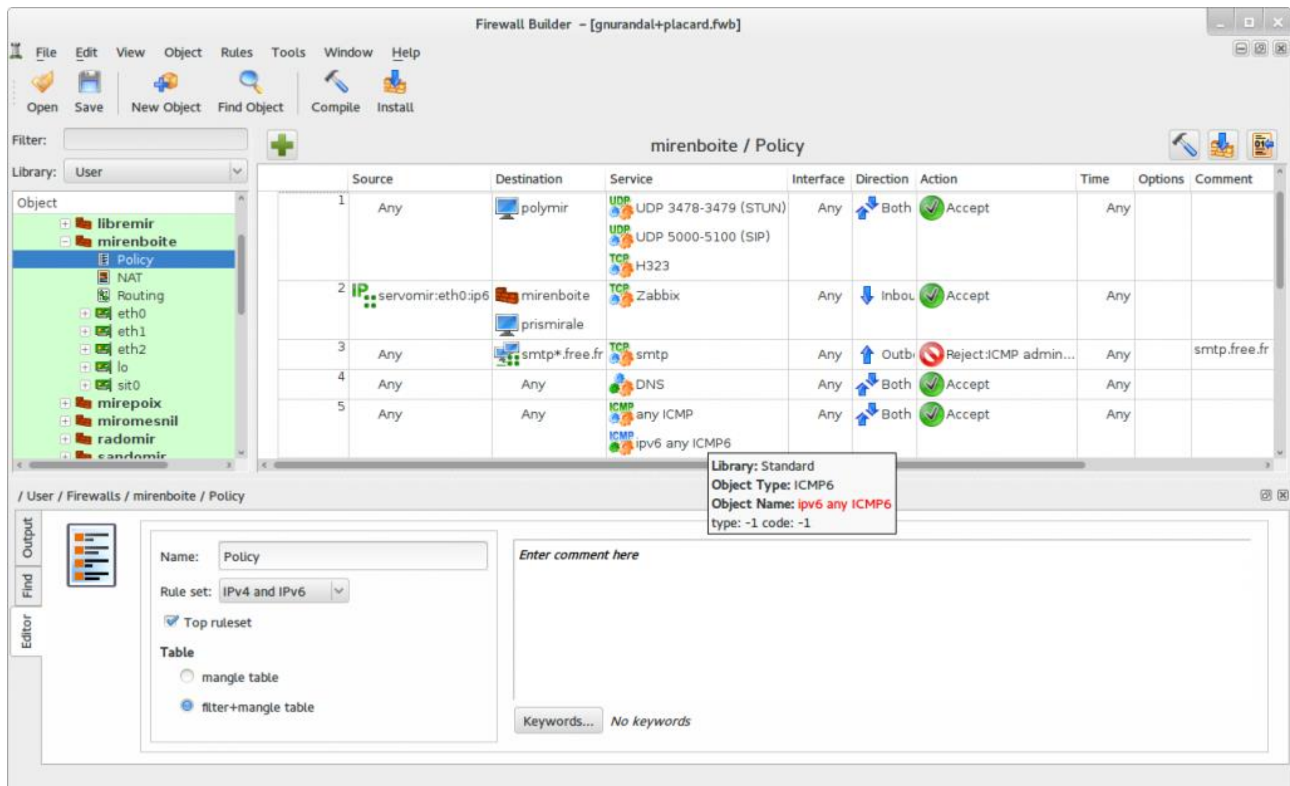
الشبكات بنطاقات IP المقابلة لها

الخوادم

المنافذ التابعة للخدمات المستضافة على الخوادم

بعد ذلك، قم بإنشاء القواعد بإجراءات السحب والإفلات البسيطة على الكائنات كما هو موضح في الشكل ٢.٧، "النافذة الرئيسية لـ Fwbuilder". يمكن لبعض القوائم السياقية تغيير الحالة (نفيها، على سبيل المثال). ثم يجب اختيار الإجراء وتكوينه.

بقدر ما يتعلق الأمر بـ IPv6، يمكنك إما إنشاء مجموعتي قواعد مميزتين لـ IPv4 و IPv6، أو إنشاء واحدة فقط والسماح لـ **fwbuilder** بترجمة القواعد وفقًا للعناوين المخصصة للكائنات.



شكل ٢.٧، "النافذة الرئيسية لـ Fwbuilder"

سيقوم **fwbuilder** بإنشاء برنامج نصي يقوم بتكوين جدار الحماية وفقًا للقواعد التي حددتها. تمنحه بنيتها المعيارية القدرة على إنشاء برامج نصية تستهدف أنظمة مختلفة بما في ذلك **`iptables`** لنظام Linux و **`ipf`** لـ FreeBSD و **`pf`** لـ OpenBSD.

٤.٤.٧. تثبيت القواعد في كل إقلاع

من أجل تنفيذ قواعد جدار الحماية في كل مرة يتم فيها تشغيل الجهاز، ستحتاج إلى تسجيل البرنامج النصي للتكوين في توجيه **up** لملف **/etc/network/interfaces**. في المثال التالي، يتم تخزين البرنامج النصي في **/usr/local/etc/arrakis.fw**.

```
auto eth0
iface eth0 inet static
    address 192.168.0.1
    network 192.168.0.0
    netmask 255.255.255.0
    broadcast 192.168.0.255
    up /usr/local/etc/arrakis.fw
```

يفترض هذا المثال أنك تستخدم **ifupdown** لتكوين واجهات الشبكة. إذا كنت تستخدم شيئًا آخر (مثل NetworkManager أو systemd-networkd)، فارجع إلى الوثائق الخاصة بها لمعرفة طرق تنفيذ برنامج نصي بعد طرح الواجهة.

٥.٧. المراقبة والتسجيل

تعد سرية البيانات وحمايتها جانبًا مهمًا من جوانب الأمن، ولكن من المهم بنفس القدر ضمان توفر الخدمات. بصفتك مشرفًا وممارسًا للأمان، يجب عليك التأكد من أن كل شيء يعمل كما هو متوقع، وتقع على عاتقك مسؤولية اكتشاف السلوك الشاذ وتدهور الخدمة في الوقت المناسب. يلعب برنامج المراقبة وتسجيل الدخول دورًا رئيسيًا في هذا الجانب من الأمان، حيث يوفر نظرة ثاقبة لما يحدث على النظام والشبكة.

في هذا القسم، سنراجع بعض الأدوات التي يمكن استخدامها لمراقبة العديد من جوانب نظام كالي.

١.٥.٧. مراقبة السجلات باستخدام logcheck

يراقب برنامج **`logcheck`** ملفات السجل كل ساعة بشكل افتراضي ويرسل رسائل سجل غير عادية في رسائل البريد الإلكتروني إلى المسؤول لمزيد من التحليل.

يتم تخزين قائمة الملفات المراقبة في /etc/logcheck/logcheck.logfiles. تعمل القيم الافتراضية بشكل جيد إذا لم يتم إصلاح الملف /etc/rsyslog.conf بالكامل.

logcheck يمكن أن يقدم تقرير تسجيل الدخول مستويات مختلفة من التفاصيل:

شكوك الخادم ومحطة العمل. وشكوك مطوّلة جدًا، وربما يجب أن يقتصر على خوادم محددة مثل: جدران الحماية. *الخادم* هو الوضع الافتراضي ويوصى به لمعظم الخوادم. من الواضح أن *محطة العمل* مصممة لمحطات العمل وهي مقتضبة للغاية، حيث تقوم بتصفية رسائل أكثر من الخيارات الأخرى.

في جميع الحالات الثلاث، ربما يجب تخصيص **logcheck** لاستبعاد بعض الرسائل الإضافية (اعتمادًا على الخدمات المثبتة)، ما لم ترغب حقًا في تلقي دفعات كل ساعة من رسائل البريد الإلكتروني الطويلة غير المثيرة للاهتمام. نظرًا لأن آلية اختيار الرسائل معقدة نوعًا ما، فإن قراءة /usr/share/doc/logcheck-database/README.logcheck-database.gz/ مطلوبة - إذا كانت صعبة - للقراءة.

يمكن تقسيم القواعد المطبقة إلى عدة أنواع:

تلك التي تعتبر رسالة كمحاولة اختراق (مخزنة في ملف في /etc/logcheck/cracking.d/directory/).

محاولات الاختراق المتجاهلة (/etc/logcheck/cracking.ignore.d/).

الرسائل المصنفة على أنها تنبيه أمان (/etc/logcheck/violations.d/).

تنبيهات الأمان التي تم تجاهلها (/etc/logcheck/violations.ignore.d/).

أخيرًا، الرسائل المتبقية (تعتبر أحداث النظام).

يتم استخدام ملفات ignore.d لتجاهل (من الواضح) الرسائل. على سبيل المثال، لا يمكن تجاهل رسالة تم وضع علامة عليها كمحاولة اختراق أو تنبيه أمان (باتباع قاعدة مخزنة في ملف **etc/logcheck/violations.d/myfile**) إلا من خلال قاعدة في ملف **/etc/logcheck/violations.ignore.d/myfile** أو ملف **/etc/logcheck/violations.ignore.d/myfile**-*extension*.

يتم دائمًا الإشارة إلى حدث النظام ما لم تنص القاعدة في أحد مجلدات **/etc/logcheck/ignore.d.{paranoid,server,workstation}/** على أنه يجب تجاهل الحدث. بالطبع، المجلدات الوحيدة التي تم أخذها في الاعتبار هي تلك التي تتوافق مع مستويات الإسهاب مساوية أو أكبر من وضع التشغيل المحدد.

٢.٥.٧. مراقبة النشاط في الوقت الحقيقي

top هي أداة تفاعلية تعرض قائمة بالعمليات الجارية حاليًا. يعتمد الفرز الافتراضي على المقدار الحالي لاستخدام المعالج ويمكن الحصول عليه باستخدام المفتاح P. تتضمن أوامر الفرز الأخرى الفرز حسب الذاكرة المشغولة (المفتاح M)، حسب إجمالي وقت المعالج (المفتاح T)، ومعرف العملية (المفتاح N). يقتل المفتاح k العملية بإدخال معرف العملية الخاص بها. يغير المفتاح r أولوية العملية.

عندما يبدو النظام مثقلاً، فإن **top** هي أداة رائعة لمعرفة العمليات التي تتنافس على وقت المعالج أو تستهلك الكثير من الذاكرة. على وجه الخصوص، من المثير للاهتمام غالبًا التحقق مما إذا كانت العمليات التي تستهلك الموارد تتطابق مع الخدمات الحقيقية التي من المعروف أن الجهاز يستضيفها. هناك عملية غير معروفة تعمل كمستخدم "www-data" يجب أن تبرز حقًا ويتم التحقيق فيها نظرًا لأنها على الأرجح نسخة من برنامج تم تثبيته وتنفيذه على النظام من خلال ثغرة أمنية في تطبيق ويب.

top أداة مرنة للغاية وتعطي الصفحة اليدوية تفاصيل حول كيفية تخصيص شاشتها وتكييفها مع احتياجاتك وعاداتك الشخصية.

gnome-system-monitor مشابهة لـ **top** وتوفر نفس الميزات تقريبًا.

٣.٥.٧. كشف التغييرات

بمجرد تثبيت النظام وتكوينه، يجب أن تظل معظم ملفات النظام ثابتة نسبيًا حتى تتم ترقية النظام. لذلك، من الجيد مراقبة التغييرات في ملفات النظام حيث أن أي تغيير غير متوقع قد يكون سببًا للقلق ويجب التحقيق فيه. يقدم هذا القسم بعضًا من الأدوات الأكثر شيوعًا المستخدمة لمراقبة ملفات النظام واكتشاف التغييرات وإعلامك اختياريًا كمسؤول عن النظام.

١.٣.٥.٧. حزم تدقيق بـ dpkg --verify

dpkg --verify (أو **dpkg -V**) هي أداة مثيرة للاهتمام لأنها تعرض ملفات النظام التي تم تعديلها (ربما من قبل مهاجم)، ولكن هذا الإخراج يجب أن يؤخذ على محمل الشك. للقيام بعملها، يعتمد dpkg على المجموع الاختباري المخزن في قاعدة البيانات الخاصة به والتي يتم تخزينها على القرص الصلب (الموجود في **/var/lib/dpkg/info/package.md5sums**). سيعدل المهاجم هذه الملفات بحيث تحتوي على المجموع الاختباري الجديد للملفات المخربة، أو سيهاجم المهاجم متقدم الحزمة الموجودة على مرآة دبيان الخاصة بك. للحماية من هذه الفئة من الهجمات، استخدم نظام التحقق من التوقيع الرقمي لـ APT (انظر القسم ٦.٣.٨، "التحقق من صحة الحزمة") للتحقق من صحة الحزم بشكل صحيح.

ما هي بصمة الملف؟

للتذكير: بصمة الإصبع هي قيمة، غالبًا رقم (على الرغم من ذلك في تدوين سداسي عشري)، يحتوي على نوع من التوقيع لمحتويات الملف. يتم حساب هذا التوقيع باستخدام خوارزمية (تكون MD5 أو SHA1 أمثلة معروفة جيدًا) تضمن بشكل أو بآخر أنه حتى أصغر تغيير في محتويات الملف سيؤدي إلى تغيير بصمة الإصبع؛ يُعرف هذا باسم "تأثير الانهيار الجليدي". ثم تعمل البصمة العددية البسيطة كاختبار عباد الشمس للتحقق مما إذا تم تغيير محتويات الملف. هذه الخوارزميات غير قابلة للعكس. بعبارة أخرى، بالنسبة لمعظمهم، فإن معرفة بصمة الإصبع لا تسمح بالعثور على المحتويات المقابلة. يبدو أن التطورات الرياضية الأخيرة تضعف من استبداد هذه المبادئ ولكن استخدامها ليس موضع تساؤل حتى الآن، حيث أن إنشاء محتويات مختلفة تعطي نفس بصمة الإصبع لا يزال يبدو مهمة صعبة للغاية.

سيؤدي تشغيل dpkg -V إلى التحقق من جميع الحزم المثبتة وسيطبع سطراً لكل ملف يفشل في التحقق. يشير كل حرف إلى اختبار على بعض بيانات التعريف المحددة. لسوء الحظ، لا يقوم dpkg بتخزين البيانات الوصفية اللازمة لمعظم الاختبارات وبالتالي سيخرج علامات استفهام لهم. حاليا فقط اختبار المجموع الاختباري يمكن أن يعطي ٥ على الحرف الثالث (عندما يفشل).

```
# dpkg -V
??5??????   /lib/systemd/system/ssh.service
??5?????? c /etc/libvirt/qemu/networks/default.xml
??5?????? c /etc/lvm/lvm.conf
??5?????? c /etc/salt/roster
```

في المثال أعلاه، يبلغ **dpkg** عن تغيير في ملف خدمة SSH قام به المسؤول للملف الذي تم حزمه بدلاً من استخدام تجاوز etc/systemd/system/ssh.service/ مناسب (والذي سيتم تخزينه أدناه **etc/** مثل أي تغيير في التكوين يجب يكون). يسرد أيضًا العديد من ملفات التهيئة (المحددة بحرف "c" في الحقل الثاني) التي تم تعديلها بشكل قانوني.

٢.٣.٥.٧. ملفات المراقبة: AIDE

تقوم أداة بيئة اكتشاف التطفل المتقدمة " Advanced Intrusion Detection Environment" (AIDE) بفحص تكامل الملف واكتشاف أي تغيير مقابل صورة مسجلة مسبقًا للنظام الصالح. يتم تخزين الصورة كقاعدة بيانات (var/lib/aide/aide.db/) تحتوي على المعلومات ذات الصلة في جميع ملفات النظام (بصمات الأصابع والأذونات والطوابع الزمنية وما إلى ذلك).

يمكنك تثبيت AIDE عن طريق تشغيل **apt update** متبوعًا بـ **apt install aide**. ستقوم أولاً بتهيئة قاعدة البيانات باستخدام **aideinit**، سيتم تشغيله يوميًا (عبر البرنامج النصي /etc/cron.daily/aide) للتحقق من عدم تغير أي شيء ذي صلة. عندما يتم الكشف عن التغييرات، يقوم AIDE بتسجيلها في ملفات السجل (/var/log/aide/*.log) ويرسل نتائجها إلى المسؤول عن طريق البريد الإلكتروني.

حماية قاعدة البيانات

نظرًا لأن AIDE تستخدم قاعدة بيانات محلية لمقارنة حالات الملفات، فإن صحة نتائجها ترتبط مباشرةً بصحة قاعدة البيانات. إذا حصل المهاجم على أذونات الجذر لنظام مخترق، فسيكون قادرًا على استبدال قاعدة البيانات وتغطية مساراته. تتمثل إحدى طرق منع هذا التخريب في تخزين البيانات المرجعية على وسائط تخزين للقراءة فقط.

يمكنك استخدام الخيارات في **/etc/default/aide** لتعديل سلوك الحزمة المساعدة. يتم تخزين تكوين AIDE المناسب في **/etc/aide/aide.conf** و **/etc/aide/aide.conf.d/** (في الواقع، يتم استخدام هذه الملفات فقط من خلال **update-aide.conf** لإنشاء **/var/lib/aide/aide.conf.autogenerated**). يشير التكوين إلى خصائص الملفات التي يجب التحقق منها. على سبيل المثال، تتغير محتويات ملفات السجل بشكل روتيني، ويمكن تجاهل هذه التغييرات طالما بقيت أذونات هذه الملفات كما هي، ولكن يجب أن تكون محتويات وأذونات البرامج القابلة للتنفيذ ثابتة. على الرغم من أنها ليست معقدة للغاية، إلا أن بنية التكوين ليست بديهية بالكامل ونوصي بقراءة صفحة الدليل (5) aide.conf لمزيد من التفاصيل.

يتم إنشاء نسخة جديدة من قاعدة البيانات يوميًا في /var/lib/aide/aide.db.new ؛ إذا كانت جميع التغييرات المسجلة شرعية، يمكن استخدامها لاستبدال قاعدة البيانات المرجعية.

Tripwire يشبه إلى حد بعيد AIDE، حتى بنية ملف التكوين هي نفسها تقريبًا. الإضافة الرئيسية التي توفرها tripwire هي آلية لتوقيع ملف التكوين بحيث لا يتمكن المهاجم من جعله يشير إلى نسخة مختلفة من قاعدة البيانات المرجعية.

يقدم **Samhain** أيضًا ميزات مشابهة بالإضافة إلى بعض الوظائف للمساعدة في الكشف عن الجذور الخفية. يمكن أيضًا نشره عالميًا على شبكة وتسجيل آثاره على خادم مركزي (بتوقيع).

checksecurity وحزم chkrootkit/rkhunter

يتكون **checksecurity** من العديد من البرامج النصية الصغيرة التي تقوم بإجراء الفحوصات الأساسية على النظام (البحث عن كلمات المرور الفارغة والملفات setuid الجديدة وما إلى ذلك) وتحذيرك إذا تم الكشف عن هذه الشروط. على الرغم من اسمه الصريح، لا يجب الاعتماد عليه فقط للتأكد من أن نظام Linux آمن.
تكتشف حزم chkrootkit و rkhunter بعض الجذور الخفية التي يمكن تثبيتها على النظام. للتذكير، هذه هي قطع من البرامج المصممة لإخفاء اختراق النظام مع الحفاظ على التحكم في الجهاز بسرية. الاختبارات ليست موثوقة بنسبة ١٠٠ في المائة ولكنها عادة ما تلفت انتباهك إلى المشاكل المحتملة.

٦.٧. ملخص

في هذا الفصل، ألقينا نظرة على مفهوم السياسات الأمنية، وأبرزنا النقاط المختلفة التي يجب مراعاتها عند تحديد مثل هذه السياسة وتحديد بعض التهديدات لنظامك ولشخصك كمحترف أمني. ناقشنا التدابير الأمنية للحاسوب المحمول وسطح المكتب بالإضافة إلى الجدران النارية وتصفية الحزم. أخيرًا، راجعنا أدوات واستراتيجيات المراقبة وأظهرنا كيفية تنفيذها بشكل أفضل للكشف عن التهديدات المحتملة لنظامك.

نصائح تلخيصية:

خصص بعض الوقت لتحديد سياسة أمنية شاملة.

إذا كنت تقوم بتشغيل Kali على خادم يمكن الوصول إليه بشكل عام، فقم بتغيير أي كلمات مرور افتراضية للخدمات التي يمكن تكوينها (انظر القسم ٣.٧، "تأمين خدمات الشبكة") وقم بتقييد وصولهم بجدار حماية (انظر القسم ٤.٧، "جدار الحماية أو تصفية الحزم") قبل إطلاقها.

استخدم **fail2ban** لاكتشاف وحظر هجمات تخمين كلمة المرور وهجمات كلمة مرور القوة الغاشمة عن بُعد.

إذا قمت بتشغيل خدمات الويب، استضفها عبر HTTPS لمنع وسطاء الشبكة من استنشاق حركة المرور الخاصة بك (والتي قد تتضمن ملفات تعريف ارتباط المصادقة).

غالبًا ما تنشأ المخاطر الحقيقية عند السفر من عميل إلى آخر. على سبيل المثال، يمكن سرقة الحاسوب المحمول أثناء السفر أو الاستيلاء عليه من قبل الجمارك. استعد لهذه الاحتمالات المؤسفة باستخدام التشفير الكامل للقرص (انظر القسم ٢.٢.٤، "التثبيت على نظام ملفات مشفر بالكامل") وفكر في ميزة **nuke** (انظر إضافة كلمة مرور Nuke لمزيد من الأمان) لحماية بيانات عملائك.

قم بتطبيق قواعد جدار الحماية (انظر القسم ٤.٧، "جدار الحماية أو تصفية الحزم") لمنع كل حركة المرور الصادرة باستثناء حركة المرور الناتجة عن وصول VPN الخاص بك. يُقصد بهذا شبكة أمان، بحيث عندما تعطل الشبكة الافتراضية الخاصة، ستلاحظها على الفور (بدلاً من العودة إلى الوصول إلى الشبكة المحلية).

قم بتعطيل الخدمات التي لا تستخدمها. يُسهل كالي القيام بذلك نظرًا لأن جميع خدمات الشبكة الخارجية معطلة افتراضيًا.

يشتمل نواة Linux على جدار الحماية **netfilter**. لا يوجد حل جاهز لتكوين أي جدار حماية، حيث تختلف متطلبات الشبكة والمستخدم. ومع ذلك، يمكنك التحكم في **netfilter** من مساحة المستخدم باستخدام أوامر **iptables** و **ip6tables**.

يراقب برنامج **logcheck** ملفات السجل كل ساعة بشكل افتراضي ويرسل رسائل سجل غير عادية في رسائل البريد الإلكتروني إلى المسؤول لمزيد من التحليل.

top هي أداة تفاعلية تعرض قائمة بالعمليات الجارية حاليًا.

يعرض **dpkg --verify** (أو **dpkg -V**) ملفات النظام التي تم تعديلها (من المحتمل من قبل مهاجم)، ولكنها تعتمد على المجموع الاختباري، والذي قد يتم تخريبه من قبل مهاجم ذكي.

تحقق أداة بيئة كشف التسلل المتقدمة (**AIDE**) من سلامة الملف وتكتشف أي تغييرات مقابل صورة مسجلة مسبقًا للنظام الصالح.

يشبه Tripwire إلى حد كبير AIDE ولكنه يستخدم آلية لتوقيع ملف التكوين، بحيث لا يتمكن المهاجم من جعله يشير إلى إصدار مختلف من قاعدة البيانات المرجعية.

ضع في اعتبارك استخدام **rkhunter** و **checkecurity** و **chkrootkit** للمساعدة في الكشف عن الجذور الخفية على نظامك.

في الفصل التالي، سنبحث في أساسيات دبيان وإدارة الحزم. ستفهم بسرعة القوة الكامنة وراء جذور ديبيان في كالي وستتعلم كيف استغل المطورون تلك القوة. كن حذرًا، الفصل التالي كثيف إلى حد ما، ولكن من المهم أن تفهم أساسيات دبيان وإدارة الحزم إذا كنت ستصبح مستخدمًا قويًا في كالي.

التمرين الأول للفصل السابع - تأمين شبكة كالي

١. حدد جميع المنافذ المفتوحة على نظام كالي الخاص بك.

٢. قم بتكوين جدار الحماية Kali الخاص بك للسماح باتصالات TCP الواردة على المنافذ 22 و 80 و 443 فقط.

٣. تحقق من حظر المنافذ الأخرى باستخدام أداة مساعدة مثل netcat.

٤. تأكد من استمرار هذه القواعد بعد إعادة التشغيل. إعادة التشغيل للتحقق!

الإجابات:

١. تحقق من المنافذ المفتوحة

```
root@kali:~# netstat -tulpen
root@kali:~# iptables -n -L INPUT
```

إذا كان لديك منافذ قمت بحظرها، أو قواعد iptables السابقة، يمكنك إسقاطها جميعًا:

```
root@kali:~# iptables -F INPUT
root@kali:~# iptables -P INPUT ACCEPT
root@kali:~# iptables -P FORWARD ACCEPT
root@kali:~# iptables -P OUTPUT ACCEPT
```

تحقق الآن لمعرفة ما إذا كان يمكنك الاتصال بالمنفذ 4444 على جهازك عن طريق تشغيل **netcat** بالطريقة التالية. لاحظ أنه في هذا التمرين، ستختلف عناوين IP الخاصة بك بالطبع:

```
root@kali:~# nc -lnvp 4444
listening on [any] 4444 ...
```

من الجهاز المضيف أو جهاز آخر، حاول الاتصال بمثيل **netcat** للاستماع. بمجرد الاتصال، اكتب بعض الأحرف، ويجب أن تظهر في مستمع Kali VM nc:

```
root@HOST_MACHINE:~#  nc -v 172.16.161.136 4444
aaaaaaaa
```

ملاحظة: إذا كنت لا ترى الأحرف التي كتبتها في مستمع Kali nc، فهناك مشكلة. احصل على حل قبل المتابعة. إذا كنت في VM، فقم بالتبديل إلى الشبكات الموصولة " bridged networking" بدلاً من NAT، إلخ حتى يعمل هذا المثال nc.

٢. قم بتكوين جدار الحماية باستخدام أوامر مشابهة لما يلي:

```
iptables -P INPUT DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT
```

تحقق الآن لمعرفة ما إذا كان يمكنك الاتصال بالمنفذ 4444 على الجهاز ذي الجدار الناري عن طريق تشغيل **netcat** بالطريقة التالية:

```
root@kali:~# nc -lvp 4444
listening on [any] 4444 ...
```

٣. من الجهاز المضيف، حاول الاتصال بمثيل **netcat** للاستماع. يجب أن تفشل:

```
root@HOST_MACHINE:~# nc -v 172.16.161.136 4444
nc: connectx to 172.16.161.136 port 4444 (tcp) failed: Operation timed out
```

٤. الآن ، قم بإنشاء برنامج نصي iptables من هذه القواعد:

```
root@kali:~# iptables-save  > /usr/local/etc/myconfig.fw
```

وتسجيل البرنامج النصي للتكوين في التوجيه المسبق لملف /etc/network/interfaces. إعادة التشغيل لمعرفة ما إذا كانت القواعد لا تزال قائمة!

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
pre-up iptables-restore < /usr/local/etc/myconfig.fw
```

التمرين الثاني للفصل السابع – مراقبة خوادم كالي

١. قم بتثبيت **logcheck** على مثيل Kali الخاص بك

٢. جرّب استخدام خدمة SSH الخاصة بك، واكتشف ما إذا كان فحص السجل يلتقط ذلك، ويبلغ عن الهجوم.

٣. قم بإنشاء نسخة cron’ed من **logcheck**، بحيث يتم تشغيله مرة واحدة في الساعة، وإنشاء ملف سجل في /data/$(date-time).log

الإجابات:

١. قم بتثبيت **logcheck** وشغله للمرة الأولى:

```
apt-get install logcheck
sudo -u logcheck logcheck –o
```

٢. قم بتنزيل قائمة كلمات المرور، وقم بإجبار خدمة SSH الخاصة بك باستخدام hydra، وتحقق من أن تسجيل الدخول يقوم بالإبلاغ عنها:

```
wget
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/500-worst-passwords.txt
hydra -l root -P 500-worst-passwords.txt 127.0.0.1 ssh
tail -f /var/log/auth.log
sudo -u logcheck logcheck –o
```

٣. بعد ذلك، اكتب نص برمجي Bash مشابه لما يلي:

```
mkdir -p /data/
sudo -u logcheck logcheck -o > /data/$(date +"%m-%d-%Y-%T").log
```

اجعله قابل للتنفيذ وأفلته في /etc/cron.hourly.

التمرين الثالث للفصل السابع - تأمين نظام الملفات

قم بتثبيت **tripwire** على جهاز Kali الخاص بك. راقب المجلد /var/www/html للتعرف على التغييرات.

إذا فعلت كل شيء بشكل صحيح، فستحصل على الكثير من "أخطاء نظام الملفات". هل أنت hax0red؟ في كلتا الحالتين، قم بإصلاحه.

الإجابات:

١. قم بتثبيت tripwire وتكوين الملفات التي تريد حمايتها:

apt-get install tripwire # yes, yes, yes, yes

nano /etc/tripwire/twpol.txt # list the directories and files you want to protect

أضف كتلة التعليمات البرمجية التالية في ملف سياسة **tripwire**:

```
# Webserver file and folder monitoring
(
  rulename = "Web server file and directories",
  severity = $(SIG_HI)
)
{
        /var/www/html    -> $(SEC_BIN);
}
```

تحقق الآن من أن tripwire يتم التقاط أي تغييرات في var/www/html:

```
twadmin -m P /etc/tripwire/twpol.txt #Create Policy File
tripwire --init #Initialize database
tripwire --check #Initial integrity check
touch /var/www/html/shell_backdoor.php
tripwire --check
tripwire --update-policy -Z low /etc/tripwire/twpol.txt
tripwire --check
```

٢. السر موجود في ملف سياسة etc/tripwire/twpol.txt/. امسح السطور التي تقوم بإظهار الأخطاء. اعتبارًا من وقت كتابة هذا التقرير، قد تتضمن الملفات:

- /etc/rc.boot
- /root/mail
- /root/Mail
- /root/.xsession-errors
- /root/.xauth
- /root/.tcshrc
- /root/.sawfish
- /root/.pinerc

- /root/.mc
- /root/.gnome_private
- /root/.gnome-desktop
- /root/.gnome
- /root/.esd_auth
- /root/.elm
- /root/.cshrc
- /root/.bash_profile
- /root/.bash_logout
- /root/.amandahosts
- /root/.addressbook.lu
- /root/.addressbook
- /root/.Xresources
- /root/.Xauthority

بمجرد تغيير هذا الملف، يجب عليك تحديث ملف السياسة وتشغيل الفحص مرة أخرى:

```
tripwire --update-policy -Z low /etc/tripwire/twpol.txt
#Update Policy File
tripwire --check
```

غذاء الفكر

إليك استخدام رائع ومثير للاهتمام من **iptables**. يمكنك تحويل أي حاسوب بواجهة لاسلكية إلى نقطة وصول لاسلكية بـ **hostapd**. يأتي هذا الحل من هنا:

```
iptables -t nat -F
iptables -F
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
echo '1' > /proc/sys/net/ipv4/ip_forward
(DNS, dhcp still required)
```

أيضا، تحقق من هذا الدليل المرجعي الرائع لـ **iptables**.

https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands

اختبار الشهادة للفصل السابع

١. حدد جميع وظائف الأمان المدمجة للتثبيت الافتراضي لـ Kali Linux:

- o لم يتم تمكين أي خدمات بشكل افتراضي
- o تجزئة امتيازات الخدمة
- o تم تمكين جدار الحماية الذي تم تكوينه مسبقًا
- o تميل جميع الخدمات إلى بيانات الاعتماد غير الافتراضية

٢. أي مما يلي مرتبط بجدار حماية Kali Linux؟ اختر كل ما ينطبق.

- o netfilter
- o fwbuilder
- o ip6tables
- o iptables

٣. أي مما يلي هو سلسلة افتراضية في جدار الحماية Kali Linux؟

- o ALL
- o DROP
- o FILTER
- o INPUT
- o RAW

٤. أي من الإجراءات التالية لجدار حماية Kali Linux لن يتداخل مع الحزم التي يتم التعامل معها؟

- OUTPUT
- LOG
- ULOG
- SNAT
- ACCEPT

٥. رتب السلاسل في ترتيب المعالجة الصحيح، من الأول إلى الأخير:

- ☐ PREROUTING
- ☐ POSTROUTING
- ☐ INPUT
- ☐ FORWARD
- ☐ OUTPUT

٦. أي مما يلي سيطبق حالة خاصة من مصدر NAT على الحزم في جدار حماية Kali Linux؟

- SOURCE
- MASQUERADE
- DNAT
- POSTROUTE

٧. أي من الأوامر التالية سيمنع جميع الحزم التي تبدأ من ٨.٨.٨.٨؟

- o iptables -A OUTPUT -s 8.8.8.8 -j DROP
- o iptables -A INPUT -s 8.8.8.8 -j DROP
- o iptables -A INPUT -s 8.8.8.8 -t ALL -j DROP
- o iptables -A ALL -s 8.8.8.8 -j DROP

٨. أي من الأوامر التالية يستخدم لحذف جميع القواعد في سلسلة INPUT؟

- o iptables -X INPUT
- o iptables -F INPUT
- o iptables -D INPUT
- o iptables -R INPUT

٩. أي مما يلي سيسمح صراحة باتصالات SSH بجهاز Kali Linux؟

- o iptables -A INPUT -p ssh -j ACCEPT
- o iptables -A INPUT –dport 22 -j ACCEPT
- o iptables -A INPUT –state NEW -p tcp –dport 22 -j ACCEPT
- o iptables -A INPUT -m state –state NEW -p tcp –dport 22 -j ACCEPT

١٠. ما الملف الذي يجب تحديثه لتمكين قواعد جدار الحماية المخصصة في وقت الإقلاع؟

- /etc/netfilter.conf
- /etc/network/interfaces
- /etc/init.d/netfilter
- /etc/netfilter/netfilter.conf

١١. ما الأداة التي يمكن استخدامها لمراقبة حالة العملية رسوميا؟

- ps -ax
- System Monitor
- ntop
- gnome-system-monitor

١٢. أي أمر سهل التخريب يمكن استخدامه للكشف عن الحزم المشبوهة؟

- dpkg –V
- dpkg -l
- dpkg -v
- dpkg –checksum

١٣. أي مما يلي يمكن استخدامه للحماية من عمليات تسجيل الدخول القوة الغاشمة؟

- logcheck
- AIDE
- tripwire
- fail2ban

الإجابات:

١. لم يتم تمكين أي خدمات بشكل افتراضي
٢. كل الخيارات

3. INPUT
4. LOG, ULOG, ACCEPT.
5. PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING
6. MASQUERADE
7. iptables -A INPUT -s 8.8.8.8 -j DROP
8. iptables -F INPUT
9. iptables -A INPUT -m state –state NEW -p tcp –dport 22 -j ACCEPT
10. /etc/network/interfaces
11. gnome-system-monitor
12. dpkg -V
13. fail2ban